S. HRG. 107–989

# FBI COMPUTERS: 1992 HARDWARE—2002 PROBLEMS

## HEARING

BEFORE THE

SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

JULY 16, 2002

**Serial No. J–107–93**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
87–062 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

## COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
MARIA CANTWELL, Washington
JOHN EDWARDS, North Carolina

ORRIN G. HATCH, Utah
STROM THURMOND, South Carolina
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DeWINE, Ohio
JEFF SESSIONS, Alabama
SAM BROWNBACK, Kansas
MITCH McCONNELL, Kentucky

Bruce A. Cohen, *Majority Chief Counsel and Staff Director*
Sharon Prost, *Minority Chief Counsel*
Makan Delrahim, *Minority Staff Director*

## Subcommittee on Administrative Oversight and the Courts

CHARLES E. SCHUMER, New York, *Chairman*

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
RUSSELL D. FEINGOLD, Wisconsin
RICHARD J. DURBIN, Illinois

JEFF SESSIONS, Alabama
STROM THURMOND, South Carolina
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania

Benjamin Lawsky, *Majority Chief Counsel*
Ed Haden, *Minority Chief Counsel*

# CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESS

QUESTIONS AND ANSWERS

SUBMISSION FOR THE RECORD

# FBI COMPUTERS: 1992 HARDWARE—2002 PROBLEMS

**TUESDAY, JULY 16, 2002**

U.S. SENATE,
SUBCOMMITTEE ON ADMINISTRATIVE
OVERSIGHT AND THE COURTS,
COMMITTEE ON THE JUDICIARY,
*Washington, D.C.*

The Subcommittee met, pursuant to notice, at 2:29 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Charles E. Schumer (chairman of the subcommittee) presiding.

Present: Senators Schumer, Durbin, and Sessions.

## OPENING STATEMENT OF HON. CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Chairman SCHUMER. The hearing will come to order, and I apologize to my colleague Jeff Sessions and to all the witnesses; I was here and forgot something and so had to go all the way back.

So let me begin and thank all of you for being here and thank Jeff again for his patience. He is more patient with me than I am with him, which I appreciate.

Anyway, the events of September 11 have lit a fire under Congress, the administration, and most of our Federal agencies, especially those on the front lines in the war on terrorism.

We all agree that the problems with the FBI's technology infrastructure have taken on a new urgency since September 11. But these problems, as we know, have been around for a long time. In fact, the only difference now is that we have witnessed firsthand the horrors of terrorism. In the past, terrorism was something that mostly happened to people in other countries. We know now just how costly that attitude can be.

Over a year ago, I introduced legislation that would have established a review commission to examine the systemic and structural problems at the FBI as well as the Bureau's relationship with other law enforcement entities.

I also held a hearing in April of this year that focused on how technology and cultural issues were acting as barriers to information-sharing between our law enforcement agencies. I heard from the Department of Justice, the FBI, and the INS, who all readily and forthrightly, to their credit, acknowledge the problems they face.

The Senate Judiciary Committee has held 11 oversight hearings since June 2001 on the FBI and the Justice Department, focusing on problematic issues from technology to security to personnel. I say all this to underscore the fact that no one should think that the challenges the FBI is facing today are new ones in any way.

There are a number of new signs that the FBI is headed down the right path. In public testimony and in private meetings, Director Mueller has been blunt about the hurdles the Bureau has to clear in order to become an agency with state-of-the-art technology and with personnel who not only know how to turn on their computers but can also type, maneuver the mouse, and who can successfully use top-of-the-line hardware and software.

In reading Ms. Higgins' testimony, I was impressed by her honesty about the difficult days ahead. Ms. Higgins, your frankness and that of the Director is refreshing.

I am also happy to report that we received Ms. Higgins' testimony yesterday over email, in contrast to how we received FBI testimony 3 months ago, when the FBI had to personally deliver it on a disk, making it impossible to circulate and store it online.

For a long time, the FBI's data base warehouse was like Medusa, with over 40 data bases with separate functions operating out of the same body but totally disconnected from one another. Here are a couple of quick visuals to give you an idea of what we are talking about.

The first visual shows you the FBI's five major investigative data bases and how they look now—disconnected and disparate. The second visual shows you how the data bases will look in a post-Trilogy world—they will be interconnected and accessible.

The Trilogy system takes an enormous step forward, not only in connecting these five major investigative data bases, but also in ensuring that every agent has a desktop computer to use, that every agent knows how to use it, and that every analyst can manipulate the resources of information available at their fingertips in real time.

I do not think I have to spell out in too much depth why connecting these networks is so important for the future of law enforcement. We know now more than ever that the backbone of homeland defense is a good information-sharing and coordination system between Federal law enforcement and intelligence agencies.

If an agency cannot coordinate information and make it easily accessible, the entire house of cards will fall. We all felt the effects of this scenario on September 11, and I pray to God that we never feel it again. But if we do not fix our communication and technological woes, we could.

Dinosaur-era technology, like the painstaking process it takes for an agent to use the automated case system where an FBI agent has to make her way through 12 different functions just to store a document must be transformed into efficient, accessible, streamlined technology.

Another example of a fossil technology is the FBI's inability to search across different data bases by plugging in a couple of key words. For example, if an agent wanted to find any information available on suicide bombers, say, in the United States, he could just type in "suicide" or "bomber" or a related phase like "homicide bomber" and come up with the relevant information.

Also, the agent should be able to type in different versions of a name—that is, take my own name. If I were to spell out S-c-h-u-m-e-r, the search engine should be able to find my name regardless of whether it has been misspelled, which believe me happens all the time.

The point here is that the FBI needs technology of the new millennium—technology that has some kind of artificial intelligence so the agency does not have to pull teeth to get one piece of information.

Glenn Fine, the Inspector General of the Justice Department, said in his testimony to the committee few months ago, and I quote: “DOJ concluded that the FBI’s troubled information systems are likely to have a continuing negative impact on its ability to properly investigate crimes and analyze information throughout the FBI.”

According to the FBI, Trilogy gives the Bureau a technological foundation upon which it can build. The other components of a state-of-the-art system cannot be implemented without first implementing the critical parts of Trilogy.

My sincere hope is that under the leadership of Ms. Higgins and Director Mueller, Trilogy will be implemented soon and will fulfill its given function. If not, I fear that Inspector General Fine’s prediction will prove true—and, if true, possible disastrous.

Before I close, I want to recognize a different sort of brass tacks. The FBI saw an increase in funding of approximately 127 percent from fiscal year 2001 to fiscal year 2002 for information management, automation, and telecommunication, IMAT, which includes all Trilogy-related functions. Congress appropriated approximately $223 million in fiscal year 2001 and $507 million in fiscal year 2002. This was an enormous increase, a jump that we all understand and deem necessary.

In addition, the Senate Appropriations Committee has recommended an appropriation of $30 million for the FBI’s Information Resources Division to help implement Phase II of Trilogy in the fiscal year 2002 supplemental. The FBI has requested an additional $48 million for fiscal year 2003 for IMAT, and I expect that as Congress considers this new request, we will want to know a detailed plan for additional funding and why it is needed.

Finally, in preparation for this hearing, I spoke with many private sector groups and what they have to say about their past dealings with the FBI in terms of lack of policy guidance, a heavy bureaucracy, and a general feeling of apathy toward the need for the latest technology. I believe that things are changing at the Bureau. I have met with some of the people here and many others. And I would like to propose the idea of forming an advisory group made up of representatives from the private sector to work with the FBI on their technology development. Perhaps this group could work in conjunction with Ms. Higgins’ Office of Programs Management, and hopefully, Ms. Higgins, we can discuss that idea in today’s hearing.

When Director Mueller testified before the Judiciary Committee a few months ago, he stated that it would take 2 to 3 years from now for the Trilogy system to be up-to-snuff. To me, that is unacceptable. I, and I believe the American people, do not need another 9/11 to prove how far behind our law enforcement agencies are in their communications and technological development.

I find it impossible to believe that we cannot, for the safety of our Nation, implement Trilogy any faster. So I will be asking you some questions on this issue later in the hearing. If Trilogy is indeed the foundation upon which the FBI's technology is built, then, we need it not today and not tomorrow—we really needed it yesterday.

Again I thank the witnesses for being here, apologize for my tardiness, and call on my patient colleague, the junior Senator from Alabama.

## STATEMENT OF HON. JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA

Senator SESSIONS. Thank you, Mr. Chairman, and thank you for your interest in this important issue.

Things do happen around here often so fast that it can happen to anybody that you do have a conflict that you just cannot balance, so I certainly understand that, and I think everybody else does, too.

I will just say a few things about this subject. I remember when I was United States Attorney that an effort was made to have a computerized system for the FBI that was going to solve everybody's problems, that you could be in court and punch in the questions, and it would appear for you and all that. And I think it was done. I do not know how many millions of dollars were spent on it, but that was done.

There is a tendency today to blame errors on the computer. The computer will not work if the information is not put in. It will not work if people are not following up. So I do not know how to make vague documents for all missed; I think some of that was just a failure to read the email that was sent out and to followup in each and every field office, who probably thought they did not have anything to do with the case.

I am concerned about the money, and I am glad that you mentioned that, Mr. Chairman. This is a huge increase in money. I think we have 60-some field offices in America, and we are talking about nearly $400 million for this program. That is a lot of money for a field office. I trust that we can justify that kind of system.

We are rushing fast, we are trying to do a lot of things at once, and we have simply got to watch our expenditures in Congress. I am getting troubled by the fact that we seem to be losing discipline.

One more thing. I do believe that you should be sure to listen to agents in the field who do the daily work and will be inputting the data into this system. They have got to feel comfortable with it, it has got to meet their needs, they have got to feel comfortable relying on it, or it will not be as effective as we would like to see it. I think that is important, and in any review that you do, I want to ask about that.

Finally, I think the most dangerous thing in all of this is security. I just believe very, very strongly that any system that allows broad-based access to security information is subject to being penetrated. You have in every FBI office in America clerks and staff people and agents. We had a Hansen, for that matter, a special agent for the FBI, who was not proven reliable and betrayed his country.

So I want to know that if we make an error, it will be to keep this material contained more closely than some might like and keep it contained in a way that is very difficult for anyone to penetrate.

Thank you for having this hearing, Mr. Chairman. If we do this thing right, I think you are correct that enemy agents could be identified quicker than we ever thought possible on occasion.

Thank you.

Chairman SCHUMER. Thank you, Jeff.

Chairman SCHUMER. Now let me call our single witness here today, one witness but a very important one and we believe worth a whole hearing.

Sherry Higgins is new. I had the pleasure of meeting her when I asked Director Mueller how are we going to straighten this thing out, he had a few-words answer, but among the words he mentioned were "Sherry Higgins."

She is the project management executive in the Office of the Director at the FBI. She began her career in 1971 with AT&T. She was then assigned to Lucent Technologies after AT&T split.

Ms. Higgins has held several positions with both AT&T and Lucent, including both the Lucent Chief Information Officer and Chief Technical Officer of the Global Program and of Project Management. Most recently, she was an instructor of project management with the International Institute for Learning, and she also supported the Technology Command Center at the 2002 Salt Lake Olympic Games.

She has been industry-certified as a project management professional through the Project Management Institute since 1991. She holds master's certificates in both commercial and international project management—this biography is a mouthful—and was inducted into the International Who's Who of Professionals in 2000 and was featured in the August 2000 edition of CIO magazine.

Ms. Higgins, your entire statement will be included in the record. Please proceed as you wish.

## STATEMENT OF SHERRY HIGGINS, PROJECT MANAGEMENT EXECUTIVE, OFFICE OF THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, D.C., ACCOMPANIED BY MARK TANNER, DEPUTY CHIEF INFORMATION OFFICER

Ms. HIGGINS. Thank you.

First of all, I want to thank you for inviting me up here. I too think it is a very important issue.

I want to thank you for inviting me and for your support and for what I know will be your continued support.

I can tell from your charts that both of you have had a lot of discussion about Trilogy, and there have been a lot of things that you have heard in the past about Trilogy.

I have been with the FBI for 4 months, and I too have heard an awful lot about Trilogy. What I have said, though, and what I have instituted within the organization and the teams that I have been working with on the Trilogy project is I have been given a lot of reasons for why the FBI is where they are right now, and what I have asked people to do, though, is not to give me a history of excuses, but I will take history as lessons learned. We will figure out how not to do things in the wrong way or the way that they have been done in the past, but improve and move forward.

Presently on the Trilogy Project, I am not sure how much you understand about the way the project is actually divided, but it is between a part that they call TNC/IPC and a part that they call UAC. One thing that I probably did not put in my testimony is that surprise I had when I came to the FBI—I thought that the communications industry had a lock on acronyms, but I found out that the FBI has more than that.

The TNC/IPC side is what I call the network and the hardware, the actual PC side of it. And the UAC side is the applications side. The TNC/IPC side is projected to be completed over a year ahead of schedule. The original intent was for the program to be a 36-month schedule, and it was 36 months from the time the contract was awarded, which would have put us completing the network and the hardware side sometime in May of 2004. The projection for the network side is to complete by the first fiscal quarter of 2003, no later than the second quarter of 2003.

The UAC side, or the virtual case file side, the application side, is projected to complete on schedule. Contract was awarded in June of 2001, and 36 months from that would be June 2004.

The solution that we are implementing now, that we are designing now, that we are developing now, is significantly different from what was projected from the very beginning. So there are things in my testimony that explain that and some things that I am going to show you on a powerpoint presentation to demonstrate that.

Communications is improving within the Trilogy Project and other programs within the FBI. We are not there yet, but we are cross-pollinating information to make sure that we are partnering on all the programs that we have within the FBI.

We are focusing on the right solution, not just the fastest solution. We have a constant eye on the schedule to make sure that as we are moving down this road and we are putting in the right solution that we are looking for anywhere that we can get efficiencies and gain a faster schedule.

The future is bright; I agree with that. And the people who are surrounding the Trilogy program feel that the future is bright, and they resonate with the Director's view that the future is bright, that we are moving ahead.

On your point, Senator Sessions, one of the things that I totally align with is that we do have to have the agents' buy-in. In developing the UAC or virtual case file component, part of that is using what we call a "joint application design." That is made up of agents, analysts and support people to look at not how do you do your jobs with the tools that are existing, but what tools do you need to do your job. So that in reality, what we have gotten is buy-in from the beginning. We are asking, and we have recognized that they are the ones who are going to be using these tools.

We are not just rebuilding old applications. We are looking at a new application and pulling the best information from those five investigative applications.

Trilogy is an enterprise solution. Enterprise solutions create and facilitate change, so we are recognizing that. Part of the joint application design will be eliminating some old business process that are no longer required.

We have a positive future in our sights where we already have a plan in place to not allow Trilogy to get old and outdated; we have a plan to change that out as technology changes so that it stays current.

We are assessing the impact of not only those five applications but other applicants that we look at and determine whether those need to be included or they need to be eliminated.

The Director has established the Office of Programs Management for us to have a disciplined approach on not only the Trilogy Project but any other highly critical, high-dollar, visible project that we have is critical and will support the FBI's mission and strategy.

We as an Office of Programs Management, managing these major programs, will be accountable to you as our stakeholders and to our other stakeholders, including the end-users. We will be developing repeatable processes, we will build in quality, and we are set for the future. Trilogy is setting the standard; it is the base for us to be able to do all the things that are in our vision moving forward.

Thank you.

[The prepared statement of Ms. Higgins appears as a submissions for the record.]

Senator SESSIONS. Mr. Chairman, maybe Ms. Higgins can move to the Department of Homeland Security after this.

Chairman SCHUMER. Yes. When you finish this one, we are going to move you over to Homeland.

Did you have a presentation?

Ms. HIGGINS. Yes, I do have a quick presentation where I would like to show you the difference between today's environment and our national view—and I have been coached several times to make sure that I do not leave here without you knowing that this is a national view. And my point in saying that is——

Chairman SCHUMER. Excuse me. Could you just explain what a "notional view" is?

Ms. HIGGINS. I am getting ready to.

Chairman SCHUMER. OK.

Ms. HIGGINS. A notional view is when you have a contract, or you bring a contractor in who is also one of the people in the JAD, that joint application development session, you tell them what you need—you do not design the solution for them.

Chairman SCHUMER. I see.

Ms. HIGGINS. So that what you are going to be seeing is a view of how the agents and support people would like it to look. It will still have the same functions, but it may not look exactly like what you are going to see here.

Chairman SCHUMER. OK.

Ms. HIGGINS. The first thing we are going to do is show you—you alluded, Senator Schumer, to the 12 screens—I am just going to show you very quickly, going into FBINET, Automated Case Support, and Electronic Case File, all the things that you have to use just to upload one document.

Here are the first five screens that every agent has to go through. Anything they are going to want to do in ACS, they have to go through every, single one of these screens. Those are five mandatory screens, and they are all function key-driven; there is no mouse, no icon, no year 2000 look to it. It is all very keyboard-intensive-driven.

To actually upload a document, you then have these six additional screens that you have to go through. The very last screen, just to make one more point, is a screen that says you now have to print the document after you have uploaded, so it can go into the official system of record, because ACS is not used as a system of record.

Chairman SCHUMER. Do you then have to get out of your seat and do a backflip? [Laughter.]

Ms. HIGGINS. Yes, sir. [Laughter.]

Our future planned solution—what I am going to show you is the difference between Virtual Case File and ACS and explain the workload to you.

Here is the same thing, showing how you would enter a document into the system, be able to submit it and have it approved all in one step. An agent will submit information—for instance, an intake form—he takes down the information on the victim, the victim complaint, he submits the information, the supervisor approves it, and then it automatically goes into the electronic file. At that point, it is then able to be shared by other FBI agents or analysts who can look at that information that has just been submitted.

Over top of that, there will be a Data Mining Application——

Senator SESSIONS. In other words, they could do the interview and actually enter the data instead of taking notes, and it is immediately in the system?

Ms. HIGGINS. Absolutely, absolutely. And it can be done both ways. It can be done by not being in front of the computer, writing it down, and then, it is a lot easier to just immediately go into the system.

We will have the Data Mining Application, which I believe both of you alluded to, which will allow the agent to not only get information from the virtual case file, but those other stovepipe applications, and also be able to go out and mine information from other agencies.

What they are going to be able to do then is what the agent calls "mining for gold." They will go out and grab a bunch of the information, put it together in their analytical work box, and in that analytical work box, they are able to say, "Now I have something." They will submit that, it is approved, and it goes into the electronic case file, and it is ready to be viewed or collaborated or shared with other people within the FBI.

Chairman SCHUMER. What is the process for someone else in the FBI seeing that file under this new system?

Ms. HIGGINS. Depending on the——

Chairman SCHUMER. Do they have to get separate approval or anything like that?

Ms. HIGGINS. If they are within the FBI and they have the same level of security, their job title will drive how much of the information they will be able to see.

Chairman SCHUMER. So if I am an agent in Minneapolis, I could get hold of a file, let us say, to take another place in Phoenix?

Ms. HIGGINS. Right.

Chairman SCHUMER. Right away?

Ms. HIGGINS. Right.

Chairman SCHUMER. OK—which could not happen before, I take it.

Ms. HIGGINS. Exactly.

Chairman SCHUMER. Before, you had to get 16 different approvals, and you would virtually never get it.

Ms. HIGGINS. Exactly. And to speak to your issue of Hansen, we will have audits built into this so that you will be able to see who has been looking at my case, what other people have done what to this case, so we have audit trail there.

Senator SESSIONS. Is this the time to ask a question?

Chairman SCHUMER. Yes, why not?

Senator SESSIONS. All right. Would the memorandum from Arizona be immediately available for review by a person in Minnesota who had a similar type situation, or would the computer simply register that there was relevant information of some kind? In other words, would a memo such as the one written in Arizona and/or the one written in Minnesota—to me, both of those were pretty sensitive information, and there are a lot of people who have access to computers—FBI offices are open 24 hours; you have clerks in there and other people. I think it would be pretty easy, if you were determined over a period of time, to get somebody in there who knew how to penetrate the system.

Is there any limit on that?

Ms. HIGGINS. The first question that I think you are asking me is about being able to actually do a collaboration—will the document be there so that other agents can see that information. And yes, out of that virtual work box, the analytical work box that I explained in our earlier screen, it will be immediately available to other agents in the field.

As far as being able to hack into the system or be able to bypass security regulations, we are working with the security program—they are part of our project team—to make sure that we have built in the security as opposed to bolting it on.

So we are using industry practices and using input from the security department. We also have people from security who have come over from different agencies. So we are implementing that as we go.

Senator SESSIONS. I am just thinking about—Mr. Chairman, let us say there are people in your city—and I know how deeply you care about this and how real it is to the people of New York; it is not academic, it is very, very real—but we are out interviewing people right now, people are getting information on a confidential basis. There has been abuse over the years in my view by police and FBI agents saying, “My informant’s information is so secret, I do not ever tell anybody,” which is an overreaction in one way. But at the same time, they would be dead—there are people living in the community who are providing information this day, and if that information goes into the system and somebody identifies who they are, they will disappear tomorrow. So this is really serious about our security, not counting the potential danger in a lot of other ways.

Chairman SCHUMER. It is an interesting—Senator Sessions is right. I asked Director Mueller why things were so backward. It is my view that the FBI system, at least as of 9/11, was more rudimentary than the system that I bought my 7th grade daughter for $1,400. He said there are two reasons. One, he said the FBI always had the attitude that "We can do it better," instead of relying on all the geniuses in Silicon Valley and everybody else, they invented their own system, and they were not too good at it.

But the second reason, which is the one you bring up, is security. Obviously, you do not want a system that is simply open to everybody because of classified information, because of investigative problems, et cetera. And I guess the balance you face is to make it as accessible and as open as possible so an enterprising agent in Minnesota can get to see a lot of information that other agents have had, and at the same time, not having such information, certain sensitive information, be too accessible.

But I take it that with passwords and certain codes, you can sort of have an open system with certain blockages that you need special clearance to get to and so on.

Am I wrong about that?

Ms. HIGGINS. No; you are right.

Senator SESSIONS. I just think this has got to be given attention, because if every agent can access and input into the system, and you have one bad agent, the whole system is drained of intelligence in an exceedingly bad event.

Chairman SCHUMER. Yes; a very good point.

What do you say to that? I mean, the advantage of the internet is a two-edged sword, as we learned about 9/11. What do you say to the fact that if you get a high-up person in the system, they might be able to get every bit of information on that system and give it to an enemy? How do we deal with that? That is a very serious and good question.

Ms. HIGGINS. There are several items that I want to bring up in response to that. One is that, again, we have audits built into the system so that we can get flags, know that someone who is not at the level of a certain case to be able to work on that case—we know that someone else has been working in it.

We are also regulated so that not all information is shared so that you can protect the individuals, too. I am not going to profess to know what all of those laws and regulations are. I just know that they are there, and I am digging deep into them to try to make sure that we are making the system as flexible but as secure as it possibly can be.

As far as sharing the information or the amount of information being able to be shared or be released or someone getting into the system, technology can provide the solution, and I totally agree with you that the system is only as good as the human being who designed that system. On the other side of that, you can only protect the system—you have to look at what level of risk you are willing to assume, and that is what we are up against right now, looking at what level of risk we are willing to assume—not that there is not a solution to give all that information or to block all the information. You do not want to do one or the other. You have got to figure out that level of risk. And that is what we are working on.

Chairman SCHUMER. The fact of the matter is that a foreign agent high up in the FBI could do a lot more damage in terms of retrieving and sending information under our new system than under the old one. That is something that we have to be aware of. Is that fair to say?

Ms. HIGGINS. I think we have more control.

Chairman SCHUMER. You do?

Ms. HIGGINS. Yes, I do.

Chairman SCHUMER. It is freer and it has more controls.

Ms. HIGGINS. Yes, yes.

Chairman SCHUMER. Let us hope.

Ms. HIGGINS. And it is going to be easier to use—and we have had agents' input.

Senator SESSIONS. Well, we know that wars have been ended quickly and terminated one way or the other because of breaches in intelligence. The code-breakers in World War II and other wars have literally made the difference in who won key battles. I just do not think you can put too much emphasis on that. Frankly, I would say that the most sensitive things that are being done at the Intelligence Center of the FBI probably should be on an entirely different system in my view and should not be accessible to people around the country.

In other words, that team in my vision has always been—the team in Washington or wherever it is located will be the one to spot the patterns, spot the duplications, and give notice to the agents in the field, rather than allowing them to necessarily peruse everything that is in the system. It just looks for hot points.

Chairman SCHUMER. Do you want to keep going? Did you finish your presentation?

Ms. HIGGINS. Do you want me to just show you a couple of other things within the notional view——

Chairman SCHUMER. Yes, and then I have a few questions, and maybe Senator Durbin does.

Ms. HIGGINS. OK. Again, this is the notional view of the virtual case file. This would be the work space or the actual home page of an agent. When they walk in in the morning, they will see this. On the left-hand side are the items that are what they do every day, the frequently used activity, if you are familiar with work space on your daughter's PC.

What I want to do is show you that same intake form that we were talking about earlier and show that the information would be inputted into a screen like this, it will be mouse-driven, it will have pull-down screens so you do not have to type everything in. It gives you the capability to put in free-form comments at the bottom. What would happen here is the agent would input the information and would then submit the information to the supervisor, and the supervisor can then, from another screen, assign it to one of the agents within their squad.

What they will have there on notional view again is a list of agents within their squad, so it is a simple case of just clicking and being able to pick a particular agent and assign the work to him. What the agent will then see is their activity within their caseload.

They will be alerted to new information within their toolbox, within their caseload.

In this particular case, if you look at the very first item, they can drill down on that information to see what new has been added to their toolbox. In this particular case, they see that it is one of the last items, and there were pictures that were uploaded into the virtual case file.

Chairman SCHUMER. And that happens automatically—any time on some case, some other agent has added new information, they will get a "tickle" that says go look at it.

Ms. HIGGINS. Right. One of the things that is significant here, too, is that it is given the capability to put multimedia into the case file. Another thing that is significant about this is that the information stays resident with the file as opposed to staying in another locked are or another system of record; it is now resident with the case.

So the whole thing that I was showing you there goes back to the discussion that I was talking about business processes changing. if you look here, that is the intake form. It serves the functions in the middle, but what it is actually doing is replacing at least five different forms, handwritten information, and a printed copy that goes into an actual system of record.

Our work is investigative by nature. This shows that they are able to put in their information, and it is one of the other forms that will tell you, when you ask "What is it that I want to document?" you will be able to——

Chairman SCHUMER. This looks like pretty standard stuff.

Ms. HIGGINS [continuing]. Exactly—and you will be able to click on it, and instead of bring you up a screen, like NACS, where you have 12 screens, depending on the activity that you want to do, it is only going to bring up those screens. So it is a productivity tool.

Chairman SCHUMER. Let me ask you a couple of other questions if I could, Ms. Higgins. How about the problem—we have talked with Trilogy about getting the FBI system to talk to one another. What preparation is being made to get the FBI systems to talk to other Federal Government computer system, whether it be INS or CIA or Social Security or Border Patrol, et cetera? Is the system that you are building done with that in mind, or not? Tell me a little about that.

Ms. HIGGINS. Yes, it is. As I said before, we are setting the enterprise architecture standard for the FBI that will allow us in the future to share information with other agencies. We are making sure that we are using the actual technology that will allow us to integrate and share information with Department of Justice or the Department of Defense, CIA, whoever it is—so that we have the same type of technology, the same products, that we have data warehouses, and in some cases, we are even using the same vendor so that we will be complementary to each other.

Chairman SCHUMER. So that when this is finished in the second quarter of 2003, at least the hardware will be able, let us say, to talk to INS' computer system?

Ms. HIGGINS. We will be able to lay the plan. We are laying the foundation. The plans to be able to do that would be another program. Trilogy is laying the foundation for the enterprise architecture.

Chairman SCHUMER. I see. So you will have the hardware to do it, you will have the underlying method of doing it, but you have still got to work out the deal with each of the different agencies.

Ms. HIGGINS. Absolutely.

Chairman SCHUMER. OK. And what about similarly with our allies internationally—clearly, you are going to have more of a need to talk to them. Let me give you one example.

As you know, when it comes to fingerprints, there are two types—flat and rolled. And many of our allies have created civil fingerprint systems for travel visas and other purposes that use the flat print. INS, as I understand it, also uses the flat print.

Because of the Patriot Act, the Border Security Act, we are going to have to start running these flat prints of foreign travelers against your system for homeland security protections, the FBI system.

But from what I understand, the FBI's current finger print analysis system has something like a 40 percent error rate when it processes flat prints because it is set up to handle rolled prints which are used for criminal investigations. So batting 600 may get you into the Hall of Fame, but it is not good enough when it comes to fighting terrorism.

That is just one example of the hundreds of problems that you face, but how are we dealing with that problem?

Ms. HIGGINS. I wish I could answer that question for you. As far as the program that you are talking about and being part of that data base, the fingerprint system that you are talking about is not part of Trilogy. So what I can do is get back to you with an answer to that, but I cannot personally answer it.

Chairman SCHUMER. Does anyone else have an answer here?

Mr. TANNER. I am Mark Tanner. I am the Deputy CIO, so I have information about all of our FBI systems.

I do know something about the fingerprint system, that is the IAFIS, the Integrated Automated Fingerprint Information System. It is a 10-print system. It is a rolled fingerprint system that is used for identification of people. It is not wholly compatible with the flat fingerprint technologies, but there is a lot of research being undertaken to make those systems more compatible.

The IAFIS does, though, establish a standard for fingerprint minutiae and identification purposes which is shared with the international partners——

Chairman SCHUMER. Right, but it has a pretty high error rate, doesn't it?

Mr. TANNER. No. IAFIS, with the rolled fingerprint, has a very low error rate. It was designed to give us a 2-hour turnaround on a criminal fingerprint identification and a 24-hour civil print identification, and it is meeting those expectations. But a flat print may provide you a candidate list of persons, but it will have to go through a visual inspection to make the actual identification.

Chairman SCHUMER. It will take a lot longer, I imagine.

Mr. TANNER. It will take longer. But it is a technology that can mature.

Chairman SCHUMER. If you could, Ms. Higgins, in writing just get back to us as to how we are dealing with that issue.

Now, what about what I mentioned at the beginning—getting this private sector advisory board on board. We have just looked at corporate responsibility here, and what we found is that it is good for the accountants to have somebody else looking over their shoulder, giving them advice, to make sure they are not just in their own world, et cetera, particularly given what the old FBI mentality was, at least according to Mueller—"We can do it better, and we will do it our own way"—which did not lead to too much good.

What about the idea of some kind of private sector advisory board composed of top-level people who would really work closely with you—may even lend you people on a full-time basis for a period of time to help give suggestions for improvements. My guess is that some of these people will have come up against similar problems that you have had. Obviously, the emphasis on security is higher for the FBI than for most other places. But tell me what you think of that.

Ms. HIGGINS. I totally support it, and I know the Director supports it, too. There are plans to look at just that. We have looked at how we would do that. So I know the Director supports it, and I also support that.

Chairman SCHUMER. Could we talk about—and I will call on Senator Durbin in a minute; I have been here a long time on these questions—my constituents in New York have a personal interest in this, and when Director Mueller said it would take 3 years to get everything up and working, we said, gee whiz, we do not want to risk another horrible attack. Nobody in America—nobody in the world—does.

Now the timetable has moved up a little bit, but what are the barriers—what are the barriers to moving up the timetable further? Is it fiscal? Is it that you do not have the right personnel? Boil it down to its brass tacks. Given that this should be one of the highest priorities that America has, it is still going to take us a couple of years before both the hardware and then the application of the hardware is really working, up and available.

Did you say 2004?

Ms. HIGGINS. Yes. June 2004 will be its completion.

Chairman SCHUMER. That seems like an awfully long time given how important this is. What are the barriers, and what if anything can be done to move that timetable up?

Ms. HIGGINS. The right solution takes a longer time than just to get a solution. Let me backstep. We recognize the fact that June 2004 for the final completion date of this project is an extremely long time. There is nobody within the FBI who does not have that focus of wanting to get something into the hands of the agents as quickly as possible.

When you are looking at what it is that needs to be done as far as what is the right tool, that in itself takes time. And looking at old systems that do not have a lot of documentation—it takes time to recreate documentation just to be able to implement the new system to make sure that you have a lot of that information that is out there.

Chairman SCHUMER. But isn't that a personnel—you could hire more people to take the old documentation and update it; right?

Ms. HIGGINS. Part of it is resources, part of it is knowledge of what is existing out there to make sure that it is in there. But it is also making sure we have the right solution in place. We have people who are very focused on putting in the right solution from a standpoint of bringing in other resources that are from outside industry—that might help in some cases—but what you have really got to focus on is the right tool for the agents, so you will need to use the FBI resources and the FBI intelligence. There are very many bright people within the FBI, but this is a new solution.

Chairman SCHUMER. So it is a learning curve issue more than just about anything else?

Ms. HIGGINS. Well, it is a combination of things. It is a learning curve; it is the fact that we do not have the documentation to be able to implement the solution—for instance, to take ACS and say we know everything that is there, so only take these parts. There is documentation that is missing, so you have got to identify where the parts are.

One of the things that I was going to say, though, is that between now and June of 2004, we are looking at ways to relieve the pain so that the agents are not in pain until the first delivery in December of 2003. We are looking at putting search engines out there that will be faster and more efficient and more robust. We are looking at putting fixes—not fixes, but pain relievers, what I keep calling pain relievers—into the system to do things like be able to monitor when someone is in your cases.

We are looking at every way that we can while we are implementing the right solution to provide pain relievers along the way.

Chairman SCHUMER. I have a written question for you which I will not ask you to answer now, and then I will turn to Senator Durbin. But if I were the Director of the FBI, and I said, "You have a mandate to cut 6 months off that timetable deadline," what would you do?

I am not asking you for an answer now, but I am going to ask you that in writing, and maybe you can give us some answers.

Ms. HIGGINS. I appreciate you not asking me that, and I will explain later why.

Chairman SCHUMER. That Southern charm gets me every time.

[Laughter.]

Chairman SCHUMER. Senator Durbin?

Senator DURBIN. Southern Brooklyn.

Chairman SCHUMER. Southern Brooklyn—he knows; he has been there.

## STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Senator DURBIN. Thank you, Ms. Higgins, for joining us today. I am going to ask a series of questions, but first let me relate for a moment to a question asked by Senator Schumer.

I am serving on this Committee on the Judiciary, Governmental Affairs, and Intelligence, so I hear about this issue from many different angles, and it strikes me that there is one thing that we are overlooking, and it was raised by Senator Schumer, and that is that I think it is a great idea—and I applaud the idea—to bring in the experts to the FBI to take a look at it—can we do this better and faster, can we create something that can grow with the agency's needs. But for lack of a better word, the interoperability with other agencies is also critical.

We are considering the creation of another agency which will collect, maybe generate, intelligence data—the Department of Homeland Security—which will join four or five other agencies. The question is whether each of these agencies is designing its computers in a way that they can ultimately work together. I do not believe that any successful business would consider having separate branches with totally different computer systems that cannot communicate.

One of the things that I have thought about and that I am going to propose as part of the Department of Homeland Security is something like a Manhattan Project, where someone in the White House has the authority to take a look at the whole picture and say here is how the CIA and the FBI and the INS and all of the different agencies will have a computer system that can ultimately merge data into an effective use.

In the frustration of the arrest of Mr. Moussaoui in Minneapolis, the FBI agent who testified said, "We even thought at one point that we would break the rules and go to the CIA for information" to find out what was going on. That was considered out of line, I guess, but from where I am sitting, she did the right thing, or at least the people involved did the right thing.

So what is being talked about in terms of coordinating all of these agencies so that there is some interoperability of the computer systems?

Ms. HIGGINS. We are having conversations with the other agencies to see how their architecture is set up. We are taking lessons learned from other agencies. We are making sure that the architecture that we are building is going to be robust and be able to—at some point in the future; the plans are not laid, the plans are not in effect yet—but the plan is to be able to do just exactly what you are talking about, that is, to make sure that we have the technology and the architecture in place that will allow us to share information.

There is a data mining/data warehousing program within the FBI that Ken Richard is program manager for. The Trilogy program is working in lockstep with both data mining and data warehousing, which gives you the capability to look at information both from within the FBI and other agencies.

Senator DURBIN. The reason I raise that—I think that has to be done, and I think there has to be someone at the highest level, perhaps at the White House, who really does have this Manhattan Project type—we are looking for a new word—but a Manhattan Project type approach——

Chairman SCHUMER. How about the Brooklyn Project? [Laughter.]

Senator DURBIN [continuing]. Well, the Brooklyn Project—you heard it here, folks—but the idea is to come up with something that coordinates these things.

For example, 6 weeks ago, I believe it was, the Attorney General announced that he had a plan to fingerprint and photograph visa-holders coming into the United States. He did not specify the number of people involved, but it is my impression that it could range as high as some 30 million visa-holders who are in the United States during the course of a year. I thought at the time that that raised an interesting Constitutional question, an interesting profiling question, an interesting law enforcement question, but it is almost laughable from a technology viewpoint to think that we have the capability to collect, process, share, evaluate millions of pieces of information about visa-holders coming in on a regular basis.

Do you think we have that capability at the FBI and the INS today?

Ms. HIGGINS. Well, first of all, are you saying INS within FBI?

Senator DURBIN. Yes.

Ms. HIGGINS. With the systems that we have right now, with just this year's photographs, I do not think we have the capability for it to be retrievable. That kind of data collection and being able to be retrievable is what we are moving to. The architecture that we are building is scalable.

Senator DURBIN. That is the way that I feel. I think that is an honest answer. And it really raises a question about why we announce something like this when we know it is over the moon—it is not going to happen.

If I am not mistaken—and maybe you or one of your colleagues can answer this—2 or 3 years ago, Congress said to the INS and to the FBI, We want you to merge your fingerprint data bases, because both collect them, and in a merged data base, we would be able to come up with a lot more usable information.

The Inspector General for the Department of Justice told us just a few weeks ago that they are still not even close to that happening. Are you familiar with that Congressional mandate and the progress on that merger at the data bases?

Ms. HIGGINS. No, I am not.

Mark, do you know anything about that? I am not familiar with IAFIS and the fingerprinting systems, and Mark obviously has some knowledge.

Mr. TANNER. I am familiar with it. It is mainly a different operational posture that we take. INS does a two-print check, and we do a 10-print check, so there are differences in the technologies that support those two operational postures. There has been a lot of work done to figure out how those things can be integrated. Right now, off the top of my head, I do not have the details of where we are on that.

Senator DURBIN. I will not put you on the spot, but it is another illustration that when we have an announcement from the Department of Justice about potentially collecting tens of millions of fingerprints and photographs of visa-holders coming into the United States, and we take a look at the real world, technology world, that you live in, we realize that it is impossible. We do not have it.

I asked someone on the Intelligence Committee at a higher level, and he said the only option is to contract this out. We cannot do this.

I think we just went through a contracting out debate over security at airports, so we would have to face that issue, too, as we get into it.

Let me ask you this, Ms. Higgins. As you take a look at the computer capabilities at the FBI today and compare it to the computer capabilities of AT&T or Lucent where you used to work, what are the most obvious things that a worker at Lucent would walk in and look at the FBI system and say, "Wait a minute—you do not have"—fill in the blank. What is missing at the FBI today?

Ms. HIGGINS. First of all, the PC technology, which we are changing out. A part of Trilogy is upgrading the laptop or the work station environment.

Another is what I alluded to about the green screen environment as opposed to a gooey-based or a mouse-driven application that people use.

One of the other glaring things is email, lack of email. We are looking at that as far as being able to do intra email. Right now, the FBI does have an email package, but when we are looking at what we will be implementing and what someone like myself coming in from the outside, if I were to look at it, I would be expecting at least a more state-of-the-art email package.

It is those kinds of things that you would see as a layman—or, not a layman—but someone from a communications company coming in.

Senator DURBIN. Do FBI computers have access to the internet?

[Pause.]

Senator DURBIN. It is taking you too long to answer.

Ms. HIGGINS. FBINET—the information that we have within the FBI—is not accessible through the internet. We are looking——

Senator DURBIN. Of course, that is good. Now, how about the other way?

Ms. HIGGINS. And it is not accessible the other way, the way that we have it planned.

Senator DURBIN. So an FBI agent working at a computer who wants to access the internet for some information in an investigation cannot do it?

Ms. HIGGINS. That is not true, that is not true. I am sorry.

Senator DURBIN. What is true?

Ms. HIGGINS. Another part that is being planned outside of the Trilogy Project is what we are calling an internet cafe. That is where they will have the capability to search for information, but because of legal ramifications, they will not be doing case information on the internet. They will be able to mine for information and then stake it and use it——

Senator DURBIN. But today, that does not exist.

Ms. HIGGINS. In some of the field offices where we have already implemented, they have some of that capability.

Senator DURBIN. All right. So it does not exist throughout the agency.

Senator Schumer asked Director Mueller at an earlier hearing about word search, and I believe the answer was that they could search for the name of a person in a file, but they could not search for a phrase like "flight training schools". Is this true?

Ms. HIGGINS. You can put multiple word searches into ACS, and that is the system that I had put before. I know that there were some questions—there are some issues within ACS and some of the systems, and the fact that you have to go into each system to do multiple searches. But because it is an older system, and because it does not ahve the robust search engine in there, there is the ability to make a mistake and not get the information back.

You can put in "flight school" and other information. I believe Mr. Collingwood explained in more detail some of the issues about how you could go down through ACS in itself and further refine your search, so you could put "flight school" or you could put "Minnesota flight school".

Senator DURBIN. The Wall Street Journal piece that was written back in July by Messrs. David Rogers and John Wolke went into some of the Bureau's case numbering systems. Does the Bureau still hand out this little blue or yellow booklet with J. Edgar Hoover's case numbering system?

Ms. HIGGINS. Right.

Senator DURBIN. And is that still being followed in the computer programs that you are constructing?

Ms. HIGGINS. As it stands today, they are, but we do not have the final system yet. We are looking at all the business processes.

Senator DURBIN. Just to show you how archaic it is, the Wall Street Journal writes that: "The system issued to every FBI agent still includes offenses relating to prohibition, white slaver, and sedition." That is not encouraging.

I have two final questions, and I will make them as fast as I can. It seems to me that if you were starting a corporation with the data challenge that we have today, and you said we will not be operational until the middle of 2004 that your investors would say, "That does not compute. If you cannot be operational in a faster period of time, then you are not going to serve our needs" and in this case, serve the needs of national security.

Mr. Dies, who testified here a couple of times, brought to my attention problems with procurement and the procurement laws of the Federal Government. I will not go into the long history about how I got involved in this, but my question to you directly is this. Are there procurement laws in the Federal Code that are stopping or slowing you from doing what you would do in the private sector to cutoff 6 months, a year, or 2 years and move more quickly into a modern system that would serve the FBI's needs?

Ms. HIGGINS. I would say yes, and I would say that things that we have had to do because of that will tie our hands in cases of putting in a faster way to procure the funds or to acquire the funds, and in one case, tie our hands in being able to deal directly with the vendors that we have.

Senator DURBIN. So if you brought in Oracle and said, "Design the system," they would be disqualified from bidding on the system.

Ms. HIGGINS. Right.

Senator DURBIN. I will tell you—I might as well put it on the record—that I went all the way up the chain from Director Muller, Attorney General Ashcroft, Vice President Cheney, to the President, and said I am prepared to put in language to waive the procurement laws. Let us get beyond this, and I will take the heat if

I am wrong, but we have got to bring in the new system. And I was stopped by—who would stop me—OMB. OMB stopped me last Decmeber and said, “No. We want you to follow procruement laws, and the people at the FBI just do not understand them.”

Now, I am going to give to you the same challenge that I gave to Mr. Dies. I want to bring you in with OMB and sit down and go through this again, beacuse time has passed, and we cannot afford anymore delay here. And if this is being caught up in some red tape and bureaucracy, it is time to put an end to it. We need to have a modern computer system.

Mr. Chairman, you have been kind to give me extra time, and I yield back.

Chairman SCHUMER. Great job.

I want to thank you, Ms. Higgins. We have these written questions, and we hope to now have our Chief Information Officer, as soon as he is i office, come before us for more questions, and we are going to keep pursuing this until things get up to snuff.

We thank you.

Ms. HIGGINS. Thank you.

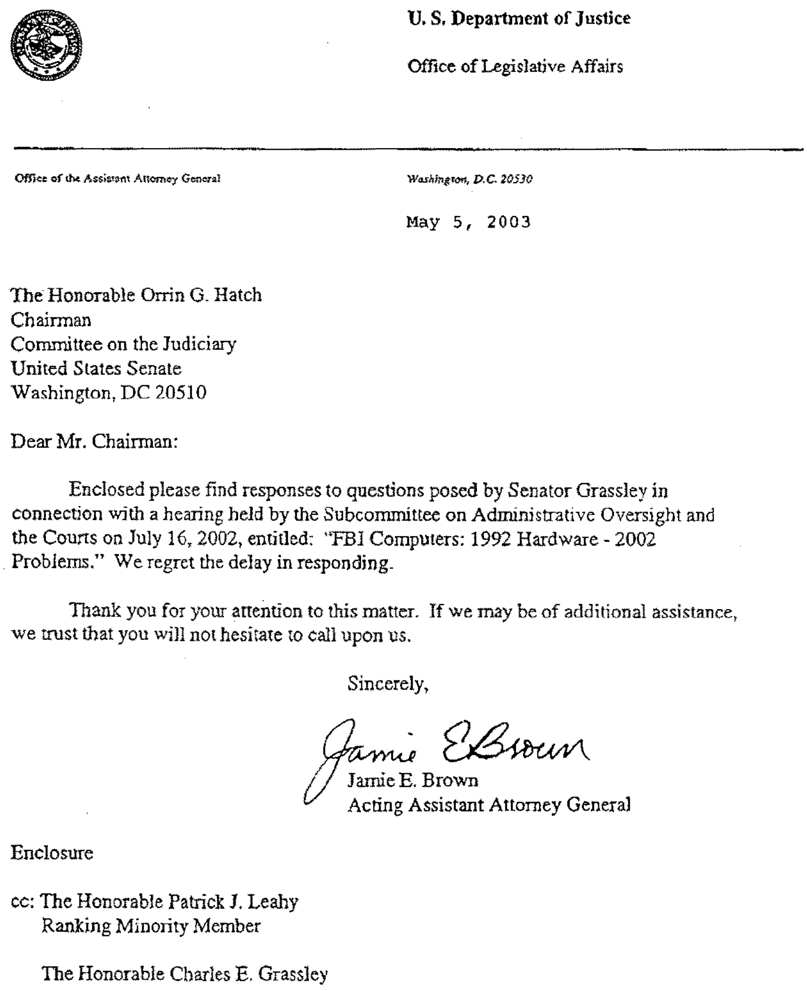
Chairman SCHUMER. I ask unanimous consent that statements of Senators Hatch and Cantwell be read into the record. Without objection.

Chairman SCHUMER. The hearing is adjourned.

[Whereupon, at 3:32 p.m., the subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

# QUESTIONS AND ANSWERS



**U. S. Department of Justice**

Office of Legislative Affairs

Office of the Assistant Attorney General

*Washington, D.C. 20530*

May 5, 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions posed by Senator Grassley in connection with a hearing held by the Subcommittee on Administrative Oversight and the Courts on July 16, 2002, entitled: "FBI Computers: 1992 Hardware - 2002 Problems." We regret the delay in responding.

Thank you for your attention to this matter. If we may be of additional assistance, we trust that you will not hesitate to call upon us.

Sincerely,

Jamie E Brown

Jamie E. Brown
Acting Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

The Honorable Charles E. Grassley

**Question #1: "What issues have facilitated the FBI's failure to upgrade its technology capabilities despite its receiving millions of dollars for such?"**

The FBI has many large complex systems addressing a number of requirements supporting our mission, as mandated by law. Over the last decade, the FBI has made substantial investments in technology for programs that support state and local law enforcement agencies, such as the National Crime Information Center (NCIC) 2000, Integrated Automated Fingerprint Identification System (IAFIS), Combined DNA Index System (CODIS), and Innocent Images. The investment of the millions of dollars in these systems has solved crimes and has assisted in apprehending the guilty and exonerating the innocent. These systems also include the National Instant Background Check System (NICS) in response to the Brady Act, developed by the FBI as an unfunded mandate. The development of some of these systems grew in cost through a variety of reasons, including increased or new requirements during their long development cycles, errors in estimation, and redesign of systems being developed on the cutting edge of technology.

At the same time, the FBI's fundamental infrastructure information technology capabilities suffered by having funding diverted to the other high priority systems. This resulted in operating with an infrastructure having no meaningful improvement for a number of years. Also contributing to this lack of improvement was the deployment of computers to additional users, including joint task forces. Networks had grown without strategic planning to support short-term critical operations, which became long-term facilities. The Trilogy Program goal is to provide FBI employees with some of the information technology tools and capabilities that are available for commercial business use today. We plan to continue to maintain the current level of technology over time.

**Question #2a: "When you said the FBI needs 'high-speed' internet, do you mean cutting-edge secure technology unparalleled by any other technologies, or do you refer to the common internet connections available to any private consumer willing to pay the monthly bill?"**

Trilogy does not provide high-speed Internet access, and FBI personnel do require the same high-speed Internet connectivity available to any private consumer. We plan to deliver this capability through a separate unclassified network as part of a non-Trilogy program called the Internet Cafe. Trilogy is intended to upgrade the internal classified network structure.

The Internet Café effort Includes $3,620,000 to expand high-speed Internet access to FBI locations. The FBI is required to provide a report to the Committees on Appropriations on the distribution and use of Internet Cafes by May 1, 2003.

**Question #2b: "In regards to the desktop environment upgrades, are these upgrades on the cutting edge of the age, or are you talking about bringing the FBI up to the level the majority of the other federal agencies was enjoying in 1995?"**

The upgrades being provided by Trilogy were the cutting edge of technology in 2001 when Trilogy was begun. With the Trilogy upgrade, provisions are being made to keep our desktop environment current, with desktops scheduled to be replaced on a three year cycle which is an industry standard.

**Question #3: "Why does the FBI need 3 years before the Trilogy can be fully implemented? More importantly, why do you think the American people can wait three years before the FBI will be ready to protect them from another terrorist threat?**

While the implementation of Trilogy is important, as it is laying a foundation for future capabilities, the FBI is not solely reliant on its completion to protect the American people from another terrorist threat. We will continue to rely on our partnerships with state, local and international law enforcement to assist us in criminal and national security investigations. There are other systems in existence or development to support these partnerships. Trilogy will upgrade infrastructure on an incremental basis, providing enhanced capabilities throughout its deployment, not only upon completion. These incremental capabilities will enable agents and analysts to work more effectively as they are deployed.

**Question #4: "What preparations have you made to facilitate the proposed transition of the NIPC to the new Department, while maintaining its effectiveness in cyber-security and prevention"**

Prior to the official transition of NIPC to the Department of Homeland Security's (DHS's) Information Analysis/Infrastructure Protection (IA/IP) Directorate on March 1st, the FBI/NIPC assigned personnel to various transition committees which shaped the new Directorate and planned for an effective transition of functions. NIPC provided numerous briefings, as well as consistency in transition planning, through several changes in IA/IP leadership. NIPC also provided personnel for the pre-March 1 DHS watch. To facilitate cyber-security and attack prevention, the FBI is currently providing IT, equipment, personnel, office space, communications, and administrative support to former NIPC elements that remain housed at FBI Headquarters.

NIPC has already been absorbed in DHS. The FBI continues to provide a wide array of support services until the DHS IA/IP leadership is established and the Directorate is fully functional.

**Question #5: "Please explain the preparations you are making to ensure that critical intelligence information can be shared as necessary with the new Department. How will the FBI's new information technology infrastructure facilitate this crucial information sharing?**

The Intelligence Counter Terrorism (CT) communication and coordination for homeland security will primarily be at the all-source Top Secret (TS) Special Compartmented Intelligence (SCI) level. Interagency communication for TS/SCI is done using the Joint Worldwide Intelligence Communications System (JWICS) backbone. Counter Terrorism intelligence information will be coordinated using CT-LINK over JWICS. Collaboration will be supported with tools such as Info Work Space (IWS) and Lotus Sametime over JWICS.

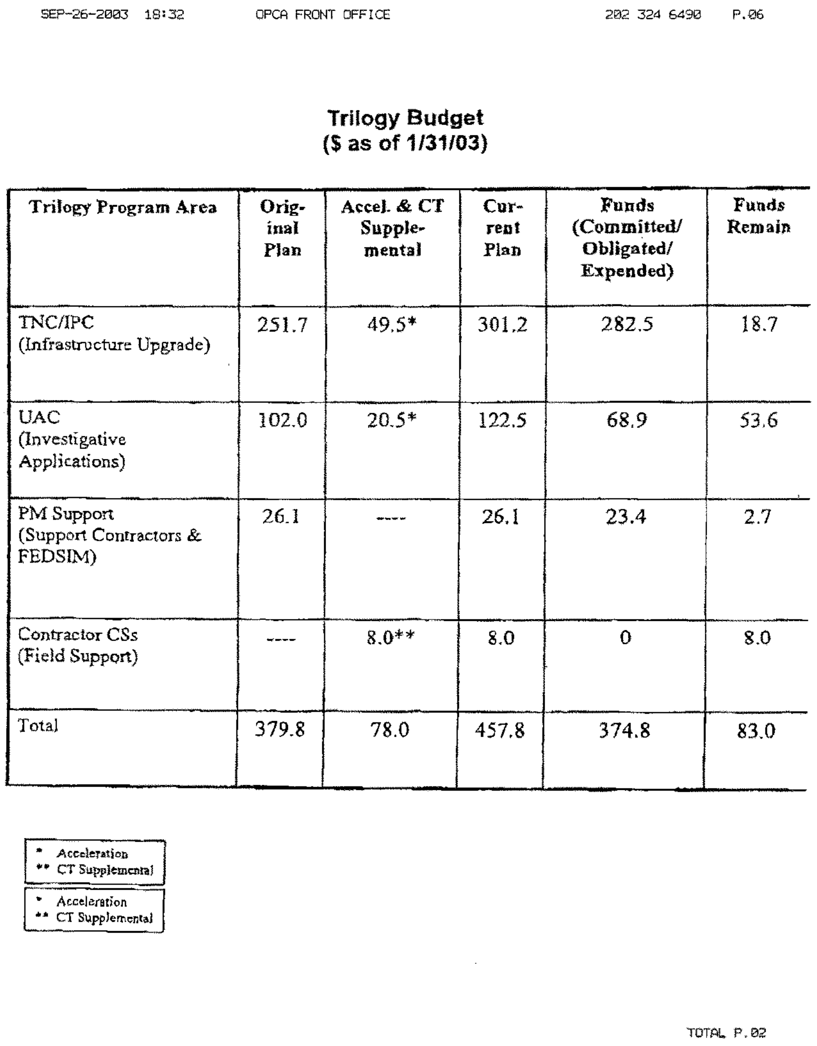
The FBI is replacing its current SCI network with a new SCI Local Area Network (LAN), wide-band connectivity to JWICS using ICMAC, new Windows 2000-based workstations, and data base/analytical tools support using the Investigative Data Warehouse (IDW) SCOPE prototype. At this time, approximately 500 workstations are connected and on-line.

Capabilities will be continually refined and upgraded using rapid spiral development over the next year. Additional data communication capabilities with Homeland Security will be available at the SECRET level using SIPRNET and at the Unclassified Sensitive level using Virtual Private Networks through Law Enforcement On-line (LEO) and the Regional Information Sharing Systems (RISS).

Intelligence support for Homeland Security will be provided through the new FBI Intelligence Office and will include support from 66 Joint Terrorist Task Forces (JTTF) and the Foreign Terrorist Tracking Task Force (FTTTF). JTTF and FTTTF communications support will be available through the use of the Trilogy Wide Area Network for both SECRET and TS/SCI. The Trilogy Transportation Network

Component/Information Presentation Component (TNC/IPC) infrastructure has 4 basic components: the Wide Area Network (WAN), the Local Area Networks (LAN), the Servers, and the hardware/software. The LAN, Servers, and hardware/software are all at the SECRET Level. The WAN has enough capacity to carry multiple channels. By separately encrypting those channels, the WAN can carry top secret/sensitive compartmented information (TS/SCI) over one channel and SECRET over another channel. The WAN was always envisioned as the primary communications medium between FBI field locations and Headquarters for all levels of traffic, separated by their own encryption. This is far more cost effective than having separate WANs. It is outside of the scope of Trilogy to provide the LAN, server, and hardware/software portion of the infrastructure for the TS/SCI support. Therefore, the FBI provided a TS/SCI LAN separately at FBI headquarters and eventually to the field.

Actual relationships with the Department of Homeland Security are still to be determined based on the final organization of the DHS Intelligence Office. Specific data exchange methods and protocols will be worked out with the new Homeland Security agency as soon as is practicable.

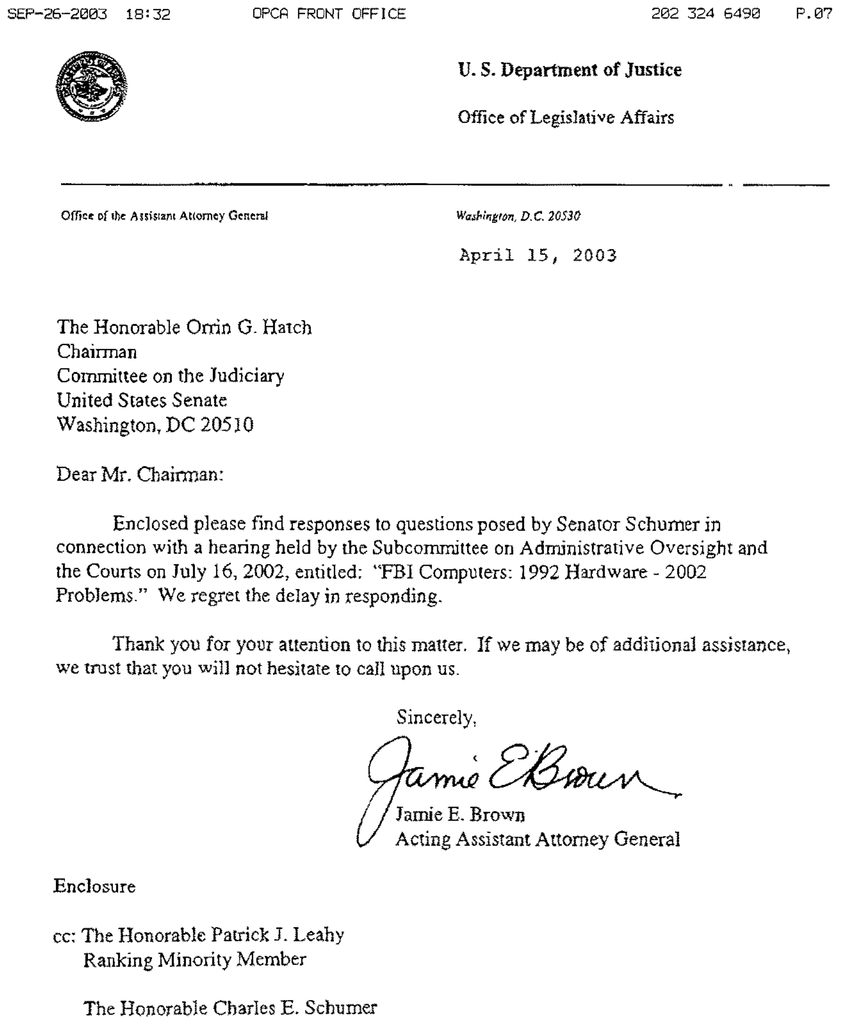


## Trilogy Budget
## ($ as of 1/31/03)

| Trilogy Program Area | Orig-inal Plan | Accel. & CT Supple-mental | Cur-rent Plan | Funds (Committed/ Obligated/ Expended) | Funds Remain |
|---|---|---|---|---|---|
| TNC/IPC<br>(Infrastructure Upgrade) | 251.7 | 49.5* | 301.2 | 282.5 | 18.7 |
| UAC<br>(Investigative Applications) | 102.0 | 20.5* | 122.5 | 68.9 | 53.6 |
| PM Support<br>(Support Contractors & FEDSIM) | 26.1 | ---- | 26.1 | 23.4 | 2.7 |
| Contractor CSs<br>(Field Support) | ---- | 8.0** | 8.0 | 0 | 8.0 |
| Total | 379.8 | 78.0 | 457.8 | 374.8 | 83.0 |

* Acceleration
** CT Supplemental

* Acceleration
** CT Supplemental



**U. S. Department of Justice**

Office of Legislative Affairs

Office of the Assistant Attorney General

*Washington, D.C. 20530*

April 15, 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions posed by Senator Schumer in connection with a hearing held by the Subcommittee on Administrative Oversight and the Courts on July 16, 2002, entitled: "FBI Computers: 1992 Hardware - 2002 Problems." We regret the delay in responding.

Thank you for your attention to this matter. If we may be of additional assistance, we trust that you will not hesitate to call upon us.

Sincerely,

Jamie E Brown

Jamie E. Brown
Acting Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

The Honorable Charles E. Schumer

### United States Senate Judiciary Committee
### Administrative Oversight and the Courts Subcommittee
### Follow-Up Questions

1. *"I believe that good information coordination will take the cooperation of management staff and technology staff. Often, I think technological staff gets pushed to the side as mere administrative personnel when they are much more of a resource. Please describe the step-by-step process you will take to ensure that this coordination takes place."*

**Response.** The FBI IT organization has attempted to balance management and technology staff resources for our development efforts. Historically, we have placed technical experts into management roles with the expectation of 'if they can do it, they can manage it'. Assessments from external and internal oversight organizations pointed out our need of professional managers to execute IT development efforts. We incorporated that recommendation into the management of our IT projects, while closely maintaining involvement of technology staff. The FBI has also consistently involved the targeted customers of IT products in their planning and development.

The newly formed Office of the Chief Information Officer (CIO) Program Management Office (PMO) will involve technology staff and customer representatives in the development of IT projects. It also enables the FBI to move away from independent stovepipe development efforts by separate divisions to an enterprise strategy for our IT development. In addition, the FBI is coordinating the development of new IT initiatives with the Department's CIO, to ensure that FBI systems are consistent with the Department's policies and architectural standards.

The process the PMO employs to ensure coordination among management staff, technology staff, customer representatives, and the Department includes the following:

Each IT project to be developed by the PMO is assigned a Project Manager from among its own staff or from the sponsoring division/organization. The Project Manager brings the requisite management skills and a degree of the technology specialty to the project. For projects being developed through a contract with the private sector (the usual case for a project meeting the criteria for PMO control), a contracting officer's technical representative (COTR) is assigned. A COTR has the technology skills and understanding of contracts to provide contractually binding technical direction to the contractor.

The PMO dedicates systems engineering resources to identify the type/level of engineering support needed on the project. Those engineering skills are drawn internally from a number of sources, to include: experienced support of legacy systems where the current project is updating a legacy system; government support engineering contractors; and specialty engineering from applicable product vendors. Engineering resources work directly with management personnel on tasks such as development of requirements documents, design, and testing plans of a contractor. Most IT projects require acceptance testing. For that, the PMO involves the technology staff in developing independent government testing of contractor-developed systems.

The PMO employs a communications coordinator, responsible for internal and external communications for each project assigned to the Office of Projects Management, ensuring a consistent and accurate message to stakeholder, user, and oversight organizations. Communications coordinated by the PMO range from completing standard reports to oversight entities, to attending user meetings of technology staffers for progress updates and interaction in question and answer sessions, to maintaining an intranet website for the presentation of project information and invite questions, to involving operations technology and product customers in requirements, prototype, pilot, and testing activities.

The PMO coordinates with the Security Division to ensure the Certification and Accreditation requirements are built into development schedules and properly monitored throughout development. In parallel the planning organization arm of the CIO will work security-engineering issues as part of the overall systems engineering architecture and requirements definition, development, and test.

The PMO ensures there is planning and execution of the transition from development to operations of the products and services developed under its control.

2. *"I think it behooves the Government to use the private sector as a model when it comes to issues like technology development. Are you aware of and do you follow industry commercial best practices as it relates to information sharing, knowledge management, and data mining? Along these lines, I will be introducing legislation to create an advisory board of private sector groups to analyze and advise the FBI and Congress on the Bureau's progress in technology development. You expressed your full support for such an idea. Can you give me some guidance on how this group would best for you in terms of what skills and expertise would be useful?"*

**Response.** At the FBI we are working to increase our awareness of IT best practices in both the private sector and other Government agencies. Recent hiring of individuals having private sector experience for key IT positions within the FBI is a first step toward increasing awareness and acceptance of best practices. Awareness of best practices and emerging IT research and development is especially important as we start developing our post-Trilogy vision for an organization-wide IT architecture.

An advisory board that is similar in composition and operation to those established at other agencies, such as the Defense Science Board and the National Oceanic and Atmospheric Administration Science Board, could certainly benefit the FBI. In developing your legislative proposal, you might want to keep in mind the following:

- The purpose of an advisory panel should be to advise the Director on the research, development, and application of existing and emerging science and technology advances and knowledge that can enable the FBI to successfully perform all aspects of our national security, criminal investigative, and law enforcement assistance missions and our support to the Intelligence Community. As such, the advisory panel should report to and be tasked by the Director.

- The panel should be structured so as to provide advice on a variety of topics and areas of interest on a continuing basis so that periodic checks can be made of multi-year IT investments by a core group of advisors. A single-focus, term-limited panel does not offer continuity in advice and perspective.

- The efforts of the panel should be focused on the pressing and complex technology problems and challenges facing the FBI. The panel should not advise on individual procurements, but rather concern itself with more strategic issues and on suggesting and assessing organizational strategies for acquiring and applying technology.

- Advisory panel members should be selected by and serve at the pleasure of the Director. Selections should be based upon preeminence in the fields of science and technology and/or accomplishment in the application of science and technology in the areas of national security and law enforcement. Technology would encompass a wide range of disciplines, such as electrical and electronic engineering; information management, exploitation, and analysis; security and information assurance; knowledge management; physics; and telecommunications.

- Panel members must be willing to consent to obtaining necessary security clearances.

An advisory panel should be provided necessary administrative, logistical, financial, security, and related support by an executive staff of FBI employees.

3. *"Have you considered performance based, managed services outsourcing including technology insertion capabilities as an effective, cost predictable way to provide support to the Bureau? If so, what functions would you consider as good candidates to be outsourced? What is your plan and when do you expect to begin outsourcing? How will you transition from Trilogy to outsourced managed services?"*

**Response.** Outsourcing has been considered, when it is appropriate, during all stages of our IT acquisition. For example, the current Trilogy development contracts were awarded as the result of a conscious decision to outsource the effort rather than attempt to perform it with FBI resources.

We are planning to outsource, using a performance-based, managed services approach, the technology refreshment program (TRP), which will replace Trilogy network and workstation hardware, network data storage, server hardware, and embedded software on a periodic basis to prevent system performance degradation and rising operations and maintenance cost due to obsolescence. The TRP also will incorporate new technology as it becomes available in the private sector and will study emerging technology to evaluate potential uses and benefits. Trilogy's TRP plans on refreshing the FBI IT infrastructure at intervals starting in FY 2004 include: 1) Servers after two years, then on a three-year cycle, 2) Work Stations and Enterprise Operations Center hardware on a three-year cycle, and 3) Network equipment on a four-year cycle. We will also evaluate ways to better anticipate our resource needs. The FBI has not yet committed to a TRP for investigative applications; however, that will be accomplished as part of a future upgrade, and will have a counter-terrorism and counter-intelligence focus. In essence, a viable infrastructure technology refreshment plan is essential to maintain the benefits of the Trilogy investment, the efficiency and capabilities of FBI investigative support systems, and to better plan and budget for out year expenditures.

Operation and maintenance of the Trilogy system is another area that will be considered for performance-based, managed services outsourcing after development is complete. Initially, the development contractor will do the operation and maintenance of Trilogy until the proper approach and vehicle is studied and the appropriate planning is complete. We have already taken the initiative to supplement the FBI Information Technology Specialists (ITS) with industry technical expertise to support them in the time of transition to Trilogy. This industry support will permit the FBI ITS to gain particular knowledge that is available from industry sources.

4. *"As you know, the FBI has a mixed history when it comes to spending its appropriations wisely when it comes to technological investments. David Walker, the Comptroller General, recently expressed concern that the FBI has not developed written policies requiring IT investments to comply with the Bureau's broad strategic plan. Why have those policies not been written and what assurances can you give us that the Trilogy Program will not suffer from the same lack of comprehensive planning that has undermined previous attempts to upgrade the Bureau's computer system?"*

**Response.** It is important to keep in mind that Trilogy is not a comprehensive plan to upgrade the FBI's 'computer system'. Trilogy is just one piece. Trilogy is not all of the FBI's investigative and intelligence applications, nor is it all of the administrative and business applications, records management, data warehousing, collaboration, or the FBI's security solution.

The written policies of IT investment management are those set in place through the guidance of the Office of Management and Budget (OMB), the General Accounting Office (GAO), and the Department of Justice. In accord with the Department's policy, the FBI's Office of the CIO plans to use the Information Technology Investment Management (ITIM) process in the management of all of the FBI's IT investments. We are currently implementing ITIM and are well on the way to having a fully functioning process.

The CIO will manage the planning, development, and operations of FBI IT investments. With those three dimensions of IT centrally attended to, the propagation of standalone, stovepipe systems should cease. In addition, the FBI will coordinate with, and report to, the Department's CIO throughout the life cycle of major FBI IT investments, such as Trilogy. The Department's CIO will confirm that FBI systems are being managed properly and are consistent with the Department's strategic goals and the Department's enterprise architecture. The Enterprise Architecture will serve as the basis for planning and evaluation of proposed IT initiatives. Reporting within the ITIM process goes through the Director, which gives IT investments more visibility and focus than they may have had in the past. The various boards of the ITIM process, the Executive Review Board, the Project Oversight Committee, and the Technical Review Board, look at all of the IT investments in the FBI's "portfolio" and strategize the big picture (their potential return on investment).

5. *"The FBI has requested an additional $48 million for its FY"03 Information Management Automation, and Telecommunications funding which includes Trilogy programs. To help Congress decide on the appropriateness of this funding request, it would be helpful to know how you intend to measure the effectiveness of Trilogy."*

**Response.** The Trilogy Program office has established a "Balanced Scorecard Metrics Report", in accordance with the Clinger-Cohen Act, to measure the initial effectiveness of Trilogy. This report is published monthly for use by Trilogy management to evaluate the success of the program and to refocus attention on areas that require greater concentration.

The effectiveness of Trilogy, through the metrics selected, is viewed from four perspectives: Customer, Internal, Growth, and Financial.

The ***Customer Perspective*** measures three factors:

1) Service Level Agreements, which evaluate, through the number of trouble tickets processed, the time it takes for corrective service, and the areas of the system affected.
2) Field Office Input, which is an annual survey of life and issues of systems and programs from the customers in the FBI's field offices. Its focus is not exclusively Trilogy, but Trilogy matters and IT needs are included in the feedback comments, and
3) End-User Participation, providing data on the level of customer interaction during requirements development, training, user conferences, etc.

The ***Internal Perspective*** measures three factors:

1) Schedule Performance during Trilogy development
2) Deployment Problem Correction, which addresses corrections after full-site capability is installed, and

3) Help Desk efficiency, which is serving a triage function during Trilogy development. Fast Track deployed desktops and peripherals, which the contractor is maintaining before Full Site Capability. Therefore, Help Desk calls are directed to internal (legacy system related) and contractor (Trilogy related) resources. Calling volume is measured, as well as time to respond and repair.

The *Growth Perspective* also measures three factors:

1) Casework efficiency, a basis for which was established using data from FYs 1999, 2000, and 2001. This will continue until Trilogy is fully functional and then serve as the baseline to measure the differences brought about with the use of the better tools of Trilogy. The number of investigative hours used to close cases will serve as the indicator.
2) Investigative Successes, which is a "soft" metric, depending on such inputs as news reports, reports to the Director during visits to field locations, etc., and
3) Training Timeliness, Participation, and Quality, which analyzes the effectiveness of training.

Finally, the ***Financial Perspective*** measures two factors:

1) Budget Performance, which monitors the funding and spend plan, and
Earned Value Management, which although a well-defined process, has lacked sufficiently hard data at this juncture to be truly effective because of the pending Engineering Change Proposals for TNC/IPC (Dyncorp) and UAC (SAIC) not yet under contract.

A "Metrics Reporting relative to Deployment Milestones" chart is maintained to show how the program has performed. An example of the chart that was included in the July report is attached.

6. *"What changes in efficiency and communication have you seen since the installation of the Trilogy architecture at your 56 Field Office locations? What problems have you encountered, what have you done to fix them, and what potential problems do you foresee?"*

**Response.** The workstations and peripherals of Trilogy have been installed at the 56 Field Office locations. The servers and networks have not been installed. The changes in efficiency and communications thus far are those that are a consequence of upgraded local equipment. Communications networks will be upgraded with Full Site Capability.

Even with the mix of Trilogy and legacy system components in the field offices, trouble calls are going to a common HELP DESK. There, a "triage" process assigns the action to investigate and correct a problem to either a legacy system established resource or a development contractor resource, as appropriate. The problems encountered with Trilogy-related equipment and service fall into the normal range of trouble calls for newly installed equipment. Response time to affect Trilogy related repairs or replacements have been a bit longer than desired, because this process was not immediately in place. Since putting the response process in place, improvement in response time has occurred. At this time, the foreseen problems are those in the normal range for the installation and initiation of a new system. To mitigate the potential for serious problems, Trilogy management is planning a pilot of operations, where representative sites of each of Trilogy's hierarchical network architecture will be 'turned on' and tested before all of Trilogy goes into operations.

7. *"Could you describe how an individual field office deals with glitches in the new Trilogy system? Does each office have a technology staffer who can assess the problem and act independently to fix it? Or do they have to consult with headquarters? Please describe the process each field office undergoes to address technical problems and solutions."*

Response: There is no "Trilogy" technology staffer in any Field Office. Following training, FBI technical staff will be accessible by phone as outlined below. We have also been training field technical specialists to develop a knowledge base from which to operate and maintain Trilogy in preparation for deployment.

There are two phases of Trilogy deployment, "Fast Track" and Full Site Capability. During "Fast Track" a field office customer experiencing potential "glitches" first contacts his/her local field office Information Technology Specialist (ITS) or Electronic Technician (ET) to verify that the problem is related to Trilogy components. If that is the case and if resolution is outside their capacity to resolve, the FBI Service Support Center (SSC) Help Desk is contacted. A ticket is logged into the "Trilogy" ticket category, as opposed to a legacy system category. Two members of the Enterprise Operations Center (EOC) staff review the Trilogy tickets and then contact the customer to resolve. If resolution is still not possible, the ticket is assigned to the DynCorp Help Desk Manager to escalate for resolution by a contractor or FBI engineer or provide maintenance replacement for the defective component.

At Full Site Capability (FSC) an Enterprise Operations Center (EOC) will be operational. There will be two EOC locations, one at Headquarters and the other at Fort Monmouth. The EOC will conduct a Site Acceptance upon completion of the FSC deployment office by office as scheduled. From that point forward the FSC field office customers will contact the EOC for problem resolution. The field office ITS and ET will contact the EOC for technical assistance if needed.

8. *"How does the FBI intend to resolve complex security clearance problems in developing the interagency links necessary for effective information sharing? The CIA, for example, operates at the security level for Top Secret-Sensitive Compartmented Information (TS-SCI) and will not share its most sensitive information on line with other agencies unless they maintain that level. The same is true of the most sensitive electronic communications intercepts from the National Security agency, which also requires security at the TS-SCI level. Does the FBI need to establish two information systems, one at the Secret level for all Special Agents and many support staff, and another at the TS-SCI level for those needing the most sensitive CIA and NSA data to work together effectively? Is Trilogy limited to information exchange between agencies at the Secret level, and if so, doesn't that dramatically reduce the ability to share highly sensitive information? What possibilities has the FBI discussed to address these security clearance problems?"*

**Response:** The purpose of Trilogy is not to provide direct information exchange with other agencies, but to upgrade the FBI's internal PC infrastructure and networks, and to develop the virtual case file. By extension, Trilogy will provide connectivity via various task forces.

The FBI has established three information systems to address mission needs for sharing information. These systems are at the Sensitive But Unclassified, Secret Collateral, and TS-SCI levels. Trilogy, the Secret system, meets a majority of FBI's internal mission needs. The TS/SCI system helps with the FBI's new mission in preventing terrorism by facilitating the exchange TS/SCI information with the Intelligence Community. This connectivity further enhances FBI's intelligence analysts' collaboration capabilities. Infrastructure savings will be realized by taking advantage of a CIA approved switch which will allow analysts to work on the TS/SCI network while using the same monitor, keyboard, and mouse for their separate Secret and TS/SCI Central Processing Units (CPUs). Further, TS/SCI information exchanged with the field will use Trilogy's wide-area network (WAN) through tunneling encryption WAN.

The Security Division (SD) has been intimately involved in all security aspects of these systems. All users of the TS/SCI information will possess a Top Secret clearance in good standing with the U.S. Government. Only those personnel with a need-to-know will be given access to TS/SCI information. Further, all users and systems administrators will be subject to a Counterintelligence-focused polygraph.

9. *"Who will be in charge of the proposed Office of Programs? Who will they report to, and how will it be funded?"*

**Response.** FBI Director Mueller established the Office of Projects Management. The Office of Projects Management is chartered to manage the FBI's projects of high value, complexity, priority, and risk during their development life cycle. The Office of Projects Management shall be led by the FBI Project Management Executive, Ms. Cheryl Z. Higgins, who will report directly to the FBI Chief Information Officer for IT projects and to the Director's designee for non-IT projects. Various funding approaches and sources are being evaluated for this office.

This office will develop, manage, and deploy high-priority, complex and high-risk projects of high dollar value, to successfully support the FBI's operational mission. The office will have a staff of subject matter experts in key program management functions, matrixed to development project managers. These project managers will be "loaned" from their sponsoring divisions to the Office of Projects Management during the development of the project, from the concept phase until the project is ready to be transitioned to operations.

In addition, the Office of Projects Management will be charged with using repeatable processes for these efforts; in other words, we will implement a business approach to our large acquisition efforts, by instituting core program management disciplines from a project's concept phase until it is transitioned to operations and maintenance. We will train a skilled corps of FBI PM subject matter experts, and advise the FBI Director on program management and acquisition planning-related organizational issues, proposals, and strategies.

Finally, the Office of Projects Management, along with the FBI's CIO, will coordinate the FBI's major IT projects with the Department's CIO to ensure that the FBI's IT investments are consistent with the Department's IT investments, architecture, and security policies and the Department's CIO satisfied that FBI IT projects are being managed appropriately.

10. *"You said in your testimony that the FBI is experiencing problems because of outdated technology. Can you explain how the FBI got so far behind technologically? Where did the FBI's current case management software originate and why was it not upgraded regularly? A 1992 Investigative Report from the House Judiciary Committee indicates the FBI may have misappropriated its case management software from the INSLAW Company and it has been suggested to me that the Bureau could not obtain standard periodic software updates from the vendor of its case management software because of that misappropriation. Is this the case?"*

**Response:** Until recently, the FBI has had little success in planning its infrastructure upgrades. Past executive leadership in the FBI was not focused on the importance of "planned obsolescence" of the FBI's networks, desktops, and investigative applications. When we finally did "get the message," the FY 1999 and FY 2000 Conference Reports directed the FBI to expend no funds, including base resources, on the FBI's technology upgrade program until Congress granted approval.

The FBI's current case management software, the Automated Case Support System (ACS), was designed and developed by the FBI using a combination of FBI computer support specialists and contract computer professionals. Using an iterative approach to system design, the FBI solicited requirements from its investigative and professional support staffs and derived software specifications. The ACS was developed using Software AG's ADABAS database management system and NATURAL programming language in the early 1990s and implemented FBI-wide in October of 1995. This system is still in use today and is updated to the extent permitted by available funding – at regular intervals. Limited upgrades and improvements have been made to ACS since 1996. ACS has implemented four releases per year containing design and interface improvements. At the time of ACS's implementation within the Bureau, there were a wide variety of computer hardware platforms in use. The FBI had desktop computers that ranged from 286 processor machines to early Pentium processors. This required that ACS be designed to accommodate the range of computers in use.

In the 1980s, representatives from the FBI visited the Executive Office of the US Attorneys (EOUSA) to see a demonstration of the INSLAW case management system. At that time the FBI realized that the system was not robust enough for the FBI, nor did it contain sufficient functionality. Therefore, FBI never implemented INSLAW's case management software.

Recognized independent experts in the computer field were retained by the DOJ to determine if any validity could be found in INSLAW's claims as represented in the 1992 House Judiciary Committee report. In every case, during every review, the experts agreed that the FBI never used, nor implemented any software designed or developed by INSLAW. The experts also determined there was no similarity between the FBI's Field Office Case Management System (FOIMS), the precursor to ACS, and in use in the FBI between 1986 and 1995, and INSLAW's system. The FBI never obtained any code from INSLAW, nor did it ever attempt to appropriate funds to purchase said code from INSLAW.

11. *"Earlier this year, Judge Webster and a group of other experts issued a report on the Hanssen espionage case that was very critical of how the Bureau safeguards information at its headquarters. In fact, the Webster Commission report expressed alarm that the Trilogy upgrade lacks key security enhancements necessary to avoid another espionage disaster. Specifically, the Commission reported that critical security measures aren't included in the Trilogy Program and will have to be integrated into the infrastructure later, a significantly more costly and less effective approach. Can you tell us what the Bureau has learned from the Hanssen case regarding its information systems and how is that knowledge being implemented as you redesign the FBI computer system?"*

**Response:** The Webster Commission's assessment that Trilogy lacks full security integration is correct. However, program planning is underway for the deployment of enterprise security solutions by the Information Assurance (IA) Program. The FBI's IA Program is working in close collaboration with Trilogy to ensure that lifecycle security solutions are deployed to meet enterprise-wide needs and to mitigate the security breech/violation caught by the Hanssen case. These enterprise security solutions will be managed and monitored by the IA Program's Enterprise Security Operations Center (ESOC). It is the IA Program's goal to ensure lifecycle security is practiced for all new systems and is exploring opportunities to integrate these solutions into the FBI's legacy systems.

12. *"If you were given a mandate to cut six months off the current timetable for full completion of Trilogy, what changes would you make and what additional resources would you need? Given unlimited resources, could you cut 12 months off the timeline?"*

**Response.** The FBI would not be able to cut six months off our current timetable and deliver the complete Trilogy infrastructure and applications functionality to our users in the field. A political mandate to reduce the schedule by twelve or six months, regardless of unlimited resources, would be difficult to achieve, and would produce questionable results. Schedule reduction would require scope reduction, rendering the product nearly useless.

A re-plan at this time would cause disruption and cost us precious time and money. We would need to balance this impact against any potential schedule savings. To reduce the schedule by twelve months, given unlimited resources, would be even less attractive, measured by return on investment in dollars or agents functionality. More specifically, from the infrastructure side, the TNC/IPC Full site Capability is currently planned for completion in March 2003, to allow the time to test and deploy a secure, operational system.

For development of investigative applications, the User Application Component (UAC), 16 months remain until completion of the initial Virtual Case File (VCF) capability. The User Application development is planned in two increments. The initial VCF release will migrate data from the current Automated Case Support (ACS) and IntelPlus to the VCF. VCF Release One has a targeted completion date of December 2003. This release will allow different types of users, such as agents, analysts, and supervisors, to access information from a "dashboard" that is specific to their individual needs. This VCF release will also enhance our capability to set and track case leads, index case information, and move document drafts more quickly through the approval process, with digital signatures.

The second release will migrate the Criminal Law Enforcement Application (CLEA), Integrated Intelligence Information Application (IIIA), and Telephone Application (TA) into the VCF. VCF Release Two has a targeted completion date estimated for June 2004. It will provide Audio/Video Streaming capability and provide our agents with "content management" capability. This will help them access information from our data warehouse, regardless of where in the system the information was entered. In order to field this system we have to be at a point where we can turn the old system off so that agents do not have to use two case management systems.

In order to turn the old system off, we have to convert complex, proprietary databases to modern ones and engineer hundreds of computer interfaces that feed the FBI from outside systems and vice versa, as well as create the software that serves our newly overhauled workflow and processes. To reduce the current timetable by six months, to ten months, we would be forced to trade schedule for a reduction in scope to shorten the critical path for VCF. The primary activities along the critical path are software integration and development; the external interfaces are security engineering, user and functional testing, data migration and agent training. The development/integration activity is the major element that drives the time required for the rest of the program.

To shorten the development and integration duration, we would need to defer significant portions of the functionality needed by the agent community and planned for VCF including features that are provided by the current systems we are replacing. We would also need to defer planned interfaces with systems internal and external to the FBI. These changes would measurably impact VCF's usability and ability to handle cases from "open to shut." FBI agents would be required to rely on paper-based operations to augment the automated case management system. Special Agents and support personnel would also be required to manually search other systems to look for case relevant information.

13. *"The Trilogy Program is a critical part of upgrading the FBI's information technology capacity but it's only a first step. In his testimony before this committee last year, Bob Dies, the former Assistant Director in charge of the FBI's Information Resources Division, stated that Trilogy, by itself, will not give the FBI a state-of-the art information system. Specifically he emphasized the need to provide better communication with other law enforcement agencies. When Trilogy is complete, will it allow the FBI to share vital data with other law enforcement offices? How will information that the FBI receives from state and local governments be incorporated into Trilogy or other FBI databases? If the Trilogy Program does not address interagency communication, who in the FBI is responsible for such information exchange and what are they doing to ensure the necessary systems are put in place? Please describe the policymaking procedures for how you will allow Trilogy access to other agencies within the Department of Justice and with other outside federal agencies? How will the new Department of Homeland Security, under the President's proposal, be involved in this process?"*

**Response:** Trilogy establishes a baseline of common PCs and investigative applications for agents and analysts so that the FBI can share intelligence internally. Building on this foundation, the next step is to enhance our information sharing capability with the Department of Justice and outside agencies within the Intelligence Community.

Consistent with the strategic goals of the Attorney General and the Department's enterprise architecture standards, we are setting the enterprise architecture standard for the FBI that will allow us, in the future, to share information with other agencies, including state and local law enforcement. Also, the FBI is participating in other Department efforts to improve information sharing.

We cannot completely answer the last part of this question, independent of other relevant agencies. Concerning the involvement of Department of Homeland Security, it will be necessary for all of the CIOs of the relevant investigative and intelligence agencies to determine how we will collaborate (e.g., have one large database which all users populate and access, OR have a central watch center where each agency is represented and each has its own database). However, we are working closely with the CIA and the Department of Homeland Security to implement the President's recently announced TTIC.

14. *"There will be significant new burdens placed on the IAFIS due to Homeland Security considerations, yet the IAFIS Technology Refreshment Program was designed prior to the events of September 11th. The technology refreshment program, which is already moving forward aggressively, calls for the upgrading of hardware with minimal changes to software, rather than an upgrading of the entire system including hardware and software. Software has been developed in the six years since the core IAFIS algorithms were installed that could reduce the hardware requirements and increase the processing capabilities of the IAFIS. Why is there no apparent consideration given to modifying the underlying software technology as part of this refreshment program?"*

**Response.** The FBI Criminal Justice Information Services (CJIS) Division's Technology Refreshment Program (TRP) represents a road map of necessary system modifications that will reduce the risk associated with the CJIS Division's ability to continue to provide critical law enforcement and civil services. The TRP plan is a living document that will evolve as system specifications change, as technology upgrades are implemented, and as new technologies evolve. The TRP plan is updated every year and each annual version represents a five-year plan for technical refreshment initiatives. The next update is due before the end of 2002.

Significant consideration has been given to software modifications within the TRP. Specifically, within the TRP plan the FBI has outlined a comprehensive strategy that first requires an in-depth analysis of the necessary system modifications. These comprehensive studies will address not only the need to upgrade the hardware, but will also address the need to upgrade/modify the IAFIS software. Since implementation of IAFIS, numerous software modifications have been installed and have resulted in increased system performance. For instance, improvements have been made to the accuracy of automated fingerprint searching techniques that have improved the productivity of workforce components by as much as 30 percent. These efforts will continue as the FBI strives to improve services. Recently, the FBI completed a target architecture study for the System of Systems with an incremental implementation strategy. In September 2002, the FBI also completed a study of how to improve the efficiency and effectiveness of the name check software used for the Interstate Identification Index and the National Instant Criminal Background Check System. These efforts exemplify the FBI's commitment to continually evaluate emerging hardware and software technologies.

15. *"The Border Security Act requires that by October 26, 2004, travel documents must be secured using biometric identifiers. The USA PATRIOT Act requires that the biometric measure identifier be capable of conducting background checks. Fingerprints are the only biometric that has an established background check capability. This means that fingerprints must be used on travel documents, and that the FBI must be responsible for handling the increased background check volume for foreign travelers. Do your current Technology Refreshment Program plans for the IAFIS include handling this increased volume?"*

**Response.** The current TRP plan does not specifically address the expected increase in demand that can be anticipated by newly passed legislation such as the Border Security Act and the USA Patriot Act. As mentioned previously, the TRP plan is a living document that must be revised continually to address change. In many cases this change results from improvements in technology. In other cases, programmatic changes are made necessary by external factors, such as September 11th and resultant legislation, such as the USA Patriot Act and Border Security Act. These unanticipated needs were not addressed in the most recent version of the TRP plan as its framework was in place prior to September 11th. Within the TRP plan, the FBI has addressed an expected growth in workload for the IAFIS over the next five years. The IAFIS, as delivered, had a processing capacity requirement for 62,500 fingerprints per day. With the improvements that have been made since delivery, the FBI has achieved a peak of over 81,000 fingerprints processed in one day and system capacity is now projected at 82,000. On average, IAFIS processes 47,000 fingerprints per day. Given the projected capacity and current demand for service, some growth is possible without resorting to major system redevelopment. It is noted that both criminal and civil fingerprint service requests have grown each year since IAFIS became operational.

As requirements grow, such as the anticipated increased workload and the required response times for the Border Security Act and the USA Patriot Act, and as the roles and responsibilities of the agencies involved become more clear, such as whether the biometric identifier (fingerprints, facial recognition, iris scan, etc.) of the traveler will be searched against the IAFIS or some other agencies' databases for verification purposes, the FBI, in coordination with these agencies, will aggressively pursue the personnel and non-personnel resources necessary to accommodate these new requirements.

16. *"Civil identification systems using flat prints are in place around the globe, and are designed to provide response times for identifications in fewer than ten seconds, including any delays from the queue. This is the type of system needed to process the visitors crossing our borders. Can the FBI commit to interoperability with such a system run by the INS or Homeland Security? What is the FBI doing to address the apparent compatibility problem with our current system and who is responsible for establishing the standardized data protocol necessary for sharing information like fingerprints or other biometric data?"*

**Response.** Yes, the FBI would suggest that the INS, Homeland Security Agency or any other agency with a criminal and/or civil identification mandate contact the FBI as soon as practicable to ensure their identification system is developed using standards established by the FBI, in concert with the American National Standards Institute (ANSI)/National Institute of Standards and Technology (NIST), during the development of the IAFIS. These standards include the ANSI/NIST American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo Information, Electronic Fingerprint Transmission Specifications for the exchange of data with the FBI, Image Quality Standards, Image Compression Standards, etc. The FBI has been working with NIST to establish standards for fingerprint and data exchange for many years. NIST is also currently performing studies relative to the use of flat fingerprint technology for the FBI. In addition, the FBI is currently exploring the viability of searching flat fingerprints against a large national file, such as that contained in the IAFIS. This effort is intended to determine the impact on search reliability and processing requirements. By developing new identification systems using the standards established by the FBI during the development of the IAFIS, compatibility concerns should be diminished. Greater concerns to the FBI are detailed in the response to question #15 above, such as system processing requirements and necessary response times.

17. *"The current IAFIS loses 40% of its accuracy when processing flat fingerprints as compared to traditional rolled fingerprints. Most civil fingerprint systems around the world will use flat prints. New software can handle flat prints and rolled prints without this loss of accuracy. Is the FBI considering this flat print processing capability in its current IAFIS refreshment program? When does the FBI expect to update its system to address this essential capability?"*

**Response:** The FBI has already made changes to the IAFIS to accommodate the searching of flat fingerprints against the IAFIS database of rolled impressions for civil identification purposes. For example, the state of Ohio uses the "WebCheck" to conduct criminal background checks for employment, licensing and other non-criminal justice purposes using flat fingerprint impressions. The Ohio Bureau of Criminal Identification and Investigation will begin submitting civil applicant fingerprint submissions to IAFIS via a pilot project in October 2002. This pilot, along with other on-going studies currently being performed in this arena, will help establish the open national standards, which can be used to expand the Ohio pilot concept into a national infrastructure for civil applicant background checks. These studies will also be used to make additional changes to the IAFIS to improve the flat fingerprint capabilities of IAFIS.

It should be noted that the flat print systems noted in the above question are used almost exclusively for verification purposes only, rather than for identification purposes. It should also be noted that the "Webcheck" program is limited to non-criminal justice purposes. The FBI strongly asserts that only rolled fingerprints will be maintained within the existing criminal data file. Rolled fingerprints provide additional details that have proven to be extremely valuable in the identification of fragmentary prints left at crime scenes. For example, the average usable area of a flat fingerprint is about 40% of the usable area of a rolled fingerprint, and latent examiners rely heavily on a full rolled image for successful casework. Without rolled fingerprints in the database, many crime scene prints would likely not be identified and a very valuable latent forensic criminal database search capability provided by the IAFIS would be significantly compromised. Additionally, the more area of a print available, the more minutiae can be extracted by the automated system, thus providing more accuracy.

18. *"As standard practice, countries around the world run separate law enforcement and civil identification systems. Mexico, for instance, maintains a criminal fingerprint database and is building a separate civil database for biometric passports, voter registrations cards, and consulate ID cards. Closer to home, New York State maintains an AFIS for criminals, and a separate civil fingerprint system run by the Office of Temporary and Disability Assistance (OTDA) for positively identifying public assistance recipients who are not criminals. The separation protects the privacy rights of law-abiding individuals and encourages them to participate in the program. If directed by Congress, would the current FBI IAFIS system be interoperable with a newly created civil identification system run by another federal agency (i.e. Department of Homeland Security)?"*

**Response:** Yes, barring any legal restrictions in providing the other Federal agency with the requested data. As mentioned in the response to question #16, the FBI would suggest that any agency with a criminal and/or civil identification mandate contact the FBI as soon as practicable to ensure their identification system is developed using standards established by the FBI, in concert with the ANSI/NIST, during the development of the IAFIS. As mentioned above, these standards include the ANSI/NIST American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo Information, Electronic Fingerprint Transmission Specifications for the exchange of data with the FBI, Image Quality Standards, Image Compression

Standards, etc. This will ensure that any newly created identification system will be interoperable to the FBI's IAFIS.

19. *"How does the FBI's Enterprise Architecture compare to OMB Enterprise Architecture requirements? Assuming that the Trilogy Program may eventually provide an upgraded infrastructure what is your plan to maintain a "state of the market" infrastructure?"*

**Response:** Trilogy is not intended to upgrade the FBI's entire Enterprise Architecture (EA). The EA is a bureau wide plan. It addresses more than the Trilogy program.

The FBI's EA is being developed using guidance based on the Federal Enterprise Architecture Framework and the Chief Information Officer (CIO) Council's document, "A practical Guide to Federal Enterprise Architecture." FBI EA is also being coordinated with the EA for the Department of Justice, which is being developed by the Department's CIO. Representatives of FBI's EA team participate in the CIO Council's committees and subcommittees that are active in the development and dissemination of plans for enhancements to the Federal EA Effort. All of these activities involve conformance to guidance from the Department, OMB, and GAO. The Enterprise Architecture is a plan that requires implementation to achieve the expected benefits.

The EA processes implement the plan. For example, the review of information technology projects for technical, project, security, and financial risk by a committee with representatives across the Bureau is currently an EA process that was piloted in FY02. This EA effort is being performed in an iterative or "Spiral" approach. Even though the EA is still being developed the pilot has provided significant insight into the challenges and essential elements needed in both the EA and its processes. The EA process, which was piloted, has become a standard process in the FBI. However, there is additional work that must be completed to be in compliance at maturity level four. The EA team, based on the evaluation done by the DOJ IG, will have completed requirements for maturity level three upon approval by the CIO of the updated charter of the Enterprise Architecture Technology Committee (EATC).

Recent changes in the recommended approaches to the EA framework and the added focus on E-Government initiatives and component architectures are being addressed at the FBI. The EA team and a Bureau-wide EA committee (EATC) in support of the Information Technology Investment Management (ITIM) reviews all information technology projects for compliance with the EA, technical reference model, and the available COTS products. The CIO is providing guidance that will enhance the EA effort. Senior management at FBI and the Department of Justice CIO reinforce the importance of EA and compliance with OMB Enterprise architecture requirements. The Trilogy program is a significant program, but the EA effort is more comprehensive in that it addresses all IT projects.

The information resources management staff is addressing the need to maintain a "state of the market." This goal requires a coordinated effort, which is led by the CIO, executed by the Enterprise Architecture Staff, Enterprise Architecture Technology Committee (EATC), Agent User Committee, and the Investment Technology Management (ITIM) Staff. The Enterprise Architecture Staff through a formal process will be requesting the FBI Divisions, Agent User Committee, Chief Scientist, and EATC to submit with their impact statements, requirements that are not or will not be met with the current infrastructure.

Additionally, the EA team will perform a technology study that includes "state of the market" infrastructure. The technology study is used to supplement the technical reference model, which includes the Trilogy standards and an annually updated section on current infrastructure products. The analysis of the information provided by the different groups is reviewed by the EATC. The EATC, which is chaired by the Chief Architect, identifies infrastructure requirements that must be met to perform the mission. The analysis is forwarded to the CIO, who decides what organizational element submits the necessary documentation for review by the ITIM process to obtain funding for the enhancement. This process is currently being developed and implemented by the CIO staff to ensure that the FBI maintains a state of the market infrastructure.

# SUBMISSIONS FOR THE RECORD

**STATEMENT OF SENATOR ORRIN G. HATCH**
**RANKING REPUBLICAN MEMBER**
**Before the SENATE JUDICIARY COMMITTEE**
**SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS**
**Hearing on**
**"FBI Computers: 1992 Hardware – 2002 Problems"**
**July 16, 2002**

Mr. Chairman, since the September 11 terrorist attacks, the law enforcement community has been the subject of an intense level of scrutiny, to determine, first, whether everything possible was done to prevent the attacks, and second, what, if any, reforms can now be made to increase the capability of law enforcement to prevent such attacks in the future. This analysis is a healthy process, and one that has been welcomed by virtually all of our law enforcement agencies. A significant focus of this analysis has been on the documented problems and deficiencies of the Federal Bureau of Investigation's (FBI) computer systems. Today's hearing is being held to assess the recent progress that the FBI has made in solving these problems. Specifically, we will hear about the Trilogy program which will provide the FBI offices with improved network communications and the technological foundation upon which a state-of-the-art system can be built.

I believe the Justice Department and the FBI have moved in a thoughtful, measured fashion to improve the capacity of our law enforcement institutions to detect and prevent terrorist activity. Director Mueller has done an excellent job addressing criticisms and problems identified in the reviews conducted by the Office of the Inspector General (OIG). Earlier this year, Inspector General Fine testified before this Committee about the significant weaknesses in the FBI's computer systems, which were found to be antiquated, inefficient, and badly in need of improvement. The Inspector General's conclusion that the FBI's troubled information systems were likely to have a continuing negative impact on its ability to investigate properly crimes and analyze information greatly concerned me and other members of this Committee. Given this grave prediction, I was gratified to learn what Director Mueller was doing to accelerate a major overhaul of the FBI's technology system that would better enable it to gather, analyze, and share information and intelligence. Today, we will delve deeper into the progression of this overhaul.

The Committee's sole witness today is Sherry Higgins, Project Management Executive in the Office of the Director at the FBI, who will explain what the FBI is doing to fix technology problems that have been identified by the OIG reviews, as well as by members of this Committee. She will also discuss what changes the FBI has implemented to build a collaborative information infrastructure designed to better support its mission. Ms. Higgins' extensive experience with and knowledge of the intricacies involved in project management led Director Mueller to hire her to oversee the FBI's implementation of the Trilogy program.

I remain confident that the FBI and the Department of Justice are moving in the right direction. I look forward to hearing the testimony of Ms. Higgins and to continuing to work with the Department and the Bureau to assist them in their essential mission of protecting our citizens from harm.

## Prepared Statement of Ms. Sherry Higgins Project Management Executive, Office of the Director Federal Bureau of Investigation

Good morning. I'm Sherry Higgins, the FBI's Project Management Executive for the Office of the Director. I have been asked to talk to you about how the FBI is fixing old problems and building a collaborative information infrastructure to better support our mission. I have also been asked to share with you some personal perspectives on how the FBI differs from the private sector in developing our computing infrastructure.

Today, we live in a dangerous world, where criminals and terrorists exploit advances in technology to perpetrate crimes against United States citizens and our national interests. High-speed digital and wireless communications, including the Internet, are the "tools of choice." Instant global communication has expanded traditional organized crime and allowed terrorists to operate from the remotest of areas.

These kinds of abilities helped facilitate the 9/11 attacks. In response, Director Mueller is restructuring and reshaping the FBI to better fit a new mission with different priorities and to put in place the analytical and information sharing capabilities needed in the post-9/11 environment.

A component is the information infrastructure necessary to enhance our ability to collect, store, search, retrieve, analyze and share information. Prior testimony before Congress has described the problems the FBI is experiencing because of outdated technology. Thanks to support from Congress, the FBI has embarked on the information infrastructure revitalization that I will describe today and that is well under way. A word of caution, however. The FBI's problems with information technology didn't occur over night and they won't be fixed over night either. That is because it is more important to get it right and know that we have the systems and capabilities that precisely fit our mission as well as cure past problems.

The first major step in this direction is our Trilogy Program. The Trilogy Program was designed as a 36-month effort to enhance our effectiveness through technologies that facilitate better organization, access and analysis of information.

The overall direction of the Trilogy Program is to provide all FBI offices with improved network communications, a common and current set of office automation tools, and easy-to-use, re-engineered, web-based applications. Our Trilogy system consists of 3 components:

Information Presentation Component (IPC). Hardware and software within each office to provide each employee with a current "desk top" environment and equipment.

Transportation Network Component (TNC). High-speed connections linking the offices of the FBI.

User Applications Component (UAC). Five user-specific software applications to enhance each employee's ability to access, organize and analyze information.

The Information Presentation Component relies primarily on commercial-off-the shelf (COTS) hardware and software products that provide a modern desktop environment and connectivity, thus facilitating employees' ability to input, retrieve, manipulate and present information in text, image, audio and video formats. The Information Presentation Component is replacing our antiquated computer workstations, providing an updated e-mail capability, and includes simple things like additional printers and scanners that increase productivity. This component is nearing completion.

The Transportation Network Component is simply the telecommunications network consisting of high-speed connections linking the offices of the FBI, and the hardware, software and new workstations within each office to link at high speeds the entire FBI. It will provide connectivity between FBI facilities (via a WAN) and within FBI facilities (via a LAN), so that investigative information and analysis may be shared among agents and analysts easily, accurately, rapidly and securely, and at the high data volumes our new applications support. This is nearing completion as well.

The User Application Component is replacement of user applications that will enhance our ability to access, organize and analyze information. Specifically, the Trilogy Program will migrate five investigative applications into a "Virtual Case File" (VCF), to provide user-friendly, web browser access to mission critical information. A web-based interface will enable our users to have a graphical interface with investigative information. It will eliminate the cumbersome aspects of our current system, greatly enhance our collaborative environment and go a long way towards eliminating the problems obvious from Hanssen and McVeigh.

Under the FBI's old legacy investigative information system, the Automated Case Support (ACS), users navigate with the function keys instead of the point and click method common to web based applications. Simple tasks, such as storing an electronic version of a document today, require a user to perform twelve separate functions, in a "green screen" environment. That will soon change with Trilogy. Automated workflow will allow for a streamlined process to complete tasking. Storing a document for the record will occur with a click of the mouse button. This will make investigative and intelligence information immediately available to all personnel with appropriate security.

Enhanced ad hoc reporting, online information sharing and state-of-the-art analytical tools will permit those conducting investigations and analyzing data to easily organize and filter events and trends. Representatives from our field offices who are defining the VCF user needs are also challenging current FBI business practices to improving workflow and to ensure that archaic business rules are not automated.

Multimedia functionality will allow for the storage of information in its original form. Under the old system, agents cannot store non-compatible forms of digital evidence in an electronic format, instead having to describe the evidence and indicate where the evidence is stored in a control room. Multimedia functionality will facilitate electronic storage of digital evidence and media to the investigative case file, allowing access to the information from the desktop.

Trilogy also includes an Enterprise Management System (EMS), that supports all three of the components of the Trilogy Program. The EMS will allow the FBI to configure, monitor and administer information systems and components through a central Enterprise Operations Center (EOC), with local Field Office visibility into the status of equipment at their location. The EMS will gather and provide appropriate IT system metrics for Trilogy from the operations center. EMS functions include mandatory and optional capabilities for fault, configuration, accounting, performance, and security management.

The original plan for Trilogy was development and deployment over 36 months from the date of the contract awards for the infrastructure and applications development, May and June 2001, respectively. The events of September 11, 2001 impacted many aspects of the FBI, including the Trilogy Program. The urgent need for improved information technologies prompted the Director to request that Trilogy implementation be accelerated, with emphasis on those capabilities most urgently needed to support the FBI's priority cases.

In response, Congress provided additional funding and Trilogy's network and desktop infrastructure improvements were accelerated. The resulting improvements are significant.

Infrastructure enhancements are being deployed in two phases.The first phase, called "Fast Track", is installation of Trilogy architecture at our 56 Field Office locations and as many of our Resident Agencies as can be completed before the second phase begins. This consists of new network printers, color scanners, local area network upgrades, desktop workstations, and Microsoft Office applications. By the end of April 2002, deployment at all 56 FBI Field Offices and two Information Technology Centers (ITCs) was completed. Fast Track is continuing to deploy this infrastructure to our Resident Agencies.

The second phase of infrastructure deployment is called "Full Site Capability," representing the complete infrastructure upgrade. The full upgrade will provide the wide area network connectivity together with new encryption devices to protect our data, new operating systems and servers, and new and improved e-mail capability. The WAN design also has been enhanced to eliminate possible single points of failure. Completion of this phase was moved from the accelerated date of July 2002 to March 2003 to allow additional time to test and deploy a secure, operational system.

The Enterprise Operations Center (EOC) facilities, circuit and bulk fiber installations, electronic key management system, and installation of encryptors are all on schedule.

User training on the new desktop office automation software has begun and a new training management system deployed.

The UAC component is scheduled to be delivered by January 2004, or four months ahead of the original schedule. And although the Trilogy Program is accelerating the network and desktop infrastructure ahead of applications development, there are significant benefits to modernizing the infrastructure before the upgraded applications are available. Infrastructure enhancement will immediately provide FBI field offices the high-speed connections to link with one another (and within each office) and share investigative and administrative information currently available in their legacy systems. It will provide nearly every FBI employee a modern desktop, and applications and database productivity tools, which will significantly enhance work productivity.

Further, during the interim while Trilogy UAC is under development, the FBI is enhancing some of our existing legacy systems to enable web access to certain applications. So, for example, two new capabilities are the Case Control system and Global Index Application. The Case Control system was delivered in April 2002; the Global Index Application was delivered in April 2001. The Case Control System keeps track of the location of each Counter-terrorism related hard copy file, as it is routed to our field divisions and nine scanning centers; this ensures that all files are scanned and accurate file locations maintained. The Global Index Application allows the user to search for a name, date of birth, address, and/or phone number, against four of our main investigative applications systems (ACS, IIIA, CLEA, and TA), with one query, returning basic case information.

The User Application development is now planned in two increments. The initial VCF release will migrate data from the current Automated Case Support (ACS) and IntelPlus to the VCF. VCF Release One has a targeted completion date of December 2003. This release will allow different types of users, such as agents, analysts, and supervisors, to access information from a "dashboard" that is specific to their individual needs. This VCF release will also enhance our capability to set and track case leads, index case information, and move document drafts more quickly through the approval process, with digital signatures.

The second release will migrate the Criminal Law Enforcement Application (CLEA), Integrated Intelligence Information Application (IIIA), and Telephone Application (TA) into the VCF. VCF Release Two has a targeted completion date estimated for June 2004. It will provide Audio/Video Streaming capability and provide our agents with "content management" capability. This will help them access information from our data warehouse, regardless of where in the system the information was entered. For the first time we will have a "one query does it all" capability.

The VCF Team is currently using an industry-standard process called Joint Application Development (JAD) planning, to define and prioritize the users' operational requirements. By joining the application developers with the users (agents, analyst, and support personnel), applications will be built that will reflect the items needed by these individuals to perform their jobs. This approach differs from the old way of doing business: figuring out how to do your job with the tools you already have. JAD is not a rebuild of the old system. It has brought users, designers, future systems operators together to develop applications that are operationally sound and maintainable. JAD sessions started at the end of January this year and are expected to conclude next week. Additional JAD sessions will take place as part of the process for VCF Release Two.

As with any automation project, a number of risks must be managed to a have a successful Trilogy Program deployment. The top three are all related to our aggressive deployment schedule. I believe all are manageable. They are: INC/PC and UAC test and acceptance; the enterprise operations center; and legacy system interoperability.

Before we deploy our Full Site Capability infrastructure to the field, we need to test the desktops, servers, and networks to ensure that there are no problems with our final configuration. Our current schedule allows a tight allocation of time for testing, which leaves little room for resolving potential problems. To mitigate this risk, the test team is prioritizing requirements and developing a common understanding of system acceptance test coverage, conditions, and criteria. Once identified, the plan is to test the most critical aspects of the system first, and, if necessary, continue testing the non-critical areas during initial deployments.

Our aggressive schedule also leaves little time for EOC preparations in support of the deployed infrastructure. To mitigate this risk, current available EOC staff will be trained to support the Trilogy infrastructure and additional external resources will be identified for full operational support at the start of FSC deployment. Finally, contractor personnel will be utilized to supplement government staff for network services, central systems, security and the data center.

Interoperability with legacy applications is another risk area. There is currently a lack of documentation in place that captures the old legacy system functions and operations. Therefore, the UAC team is still identifying new interfaces and modifications to existing interfaces. Our schedule allocation for engineering and testing may not be adequate for successful integration infrastructure deployment with the current applications and servers. To mitigate this risk, the test team is also prioritizing these test requirements and developing a common understanding of system acceptance test coverage, conditions and criteria.

Once we catch up to a standard PC environment, the future looks very positive. We are planning for a technology refreshment program (TRP) which will replace Trilogy network and workstation hardware, network data storage, server hardware, and embedded software on a periodic basis to prevent system performance degradation and rising O&M costs due to obsolescence. The TRP also envisions the incorporation of new technology as it becomes available in the private sector and the study of emerging technologies to evaluate potential future uses and benefits and to better anticipate future resource needs. In essence, a viable infrastructure technology refreshment plan is essential to maintain the benefits of the Trilogy investment, the efficiency and capabilities of FBI investigative support systems and to better plan and budget for out year expenditures.

I have been asked to provide my personal perspective on what I have changed since reporting to the FBI this March, and how the FBI contrasts with my experience in the private sector.

Before my arrival at the FBI, the Trilogy Program was overly focused on achieving an accelerated schedule. Although the Trilogy Program will still be brought in ahead of its original schedule, we have begun allowing for more test time to ensure we deliver a quality product to the field. Industry best practices recommend "building in quality", instead of "inspecting it in". Using quality standards and compliance up front will allow us to identify and prevent mistakes that would require expensive fixes later on down the line.

Effective communications within and without the Trilogy Program is also essential to our success. I am in the process of developing a Trilogy Communications Plan that will promote effective communications across our business enterprise, so that valuable development information is not retained in pockets.

I am also developing an integrated master schedule for the Trilogy Program, which will reflect the program's critical path, dependencies and integration tasks between our three components. We will constantly review this schedule to capitalize on efficiencies and schedule improvement opportunities.

One of the striking differences between the private sector and the FBI is the Bureau's lack of a dedicated corps of acquisition specialists with which to plan, develop and manage large projects. The FBI has many talented people with some of these requisite skills; we have pockets of expertise in program management disciplines, such as financial analysis, budgeting, contract management and system engineering, residing in different divisions. However, the FBI has operated for too long without an organization responsible for proper development business practices, which would ensure that FBI systems under development are responsive to our users' requirements.

Private industry and most government agencies recognize the advantages of instituting a project management executive with a project management office to manage complex, expensive, high-risk development efforts. According to the Gartner Group, "enterprises utilizing a project office to manage the growing complexity involved with creating or acquiring and then implementing and managing these applications have a distinct advantage over those that do not.". Perhaps the most frustrating experience I have had since coming to the FBI from private industry is trying to work information technology issues that cut across the FBI's organization. "Stove piped" communications internal to the FBI prevents information and communications flow that is required to be responsive to our users and oversight. Successful project development and implementation at the FBI requires constant and accurate communications across our entire business enterprise.

To make this a reality, I have recommended, and Director Mueller has approved of the establishment of an Office of Programs Management. This office will develop, manage, and deploy high-priority, complex and high-risk projects of high dollar value, to successfully support the FBI's operational mission. The office will have a staff of subject matter experts in key program management functions, matrixed to development project managers. These project managers will be "loaned" from their sponsoring divisions to the Office of Program Management during the development of the project, from the concept phase until the project is ready to be transitioned to operations.

In addition, the Office of Program Management will be charged with using repeatable processes for these efforts; in other words, we will implement a business approach to our large acquisition efforts, by instituting core program management disciplines from a project's concept phase until it is transitioned to operations and maintenance. We will train a skilled corps of FBI PM subject matter experts, and advise the FBI Director on program management and acquisition-planning related organizational issues, proposals, and strategies.

Because of its user/management orientation, the Office of Program Management will be in a position to make the most informed recommendations concerning tradeoffs between performance, schedule, and costs of projects, to determine the best course for return on the FBI's investment in IT. This office will also gauge the impacts of delays of delivered functionality for the field divisions and headquarters, and develop budget justifications for the acquisition of required resources to support approved systems projects.

In summary, Trilogy gives the FBI workable standards and a base it can build upon. Trilogy is being built to allow for interchanges with different systems, internal and external, so that the historical problem of “not putting the pieces together” is no longer an issue. Trilogy will provide the resources and tools the FBI needs to support investigations and the critical building blocks for future improvements. The Trilogy Program is focused on getting these critical resources to our Special Agents and field support personnel as quickly as possible.